Case number:

NAIH / 2020/952 /

NAIH / 2019/5606

Object:

decision

ex officio

starting

privacy

official

procedure

DECISION

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

Hungária Med-M Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság (address: 1132

Budapest, Csanády u. 6. B. ép. V. em. 2.) (hereinafter: Customer)

an official investigation into the data protection incident initiated on 18 July 2019

due to the circumstances revealed during the proceedings on 14 October 2019

in official proceedings

(1) finds that:

a) the Customer has not complied with the processing of personal data of natural persons

the free movement of such data and Directive 95/46 / EC

Regulation (EU) 2016/679 repealing Directive

Article 32 (1) (b) of the Data Protection Regulation),

(b) the Customer has not complied with Article 33 (1) of the General Data Protection Regulation

existing incident reporting obligation,

(c) the Customer has not complied with Article 34 (1) of the General Data Protection Regulation

with the data protection incident that has occurred

in connection with

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

inform the data subject of the fact and circumstances of the incident, the data subject

the scope of personal data and the measures taken to prevent them,

3) due to the above violation, the Customer shall be notified within 30 days from the becoming final of this decision

within

HUF 7,500,000, ie seven million to five hundred thousand forints

order to pay a data protection fine;

4) order the final decision by publishing the identification data of the data 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 / 2020/952

JUDGE. number should be referred to.

The Customer shall take the measures provided for in point 2) from the 15th day after the measure has been taken

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

Towards an authority.

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

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

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

the Authority's centralized revenue collection forint account

(10032000-01040425-00000000 Centralized direct debit).

Failure to comply with the obligation under point 2) and failure to pay the fine and the late payment allowance

In the event of payment, the Authority shall order the 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 of the application addressed to the Metropolitan Court in an administrative lawsuit

can be challenged. The emergency does not affect the time limit for bringing an action. The application to the Authority must be submitted electronically, which will forward it to the court together with the case file. The trial The application for maintenance must be indicated in the application. During the emergency, the court is hearing acting outside. For those who do not benefit from full personal exemption, the administrative lawsuit its fee is HUF 30,000, the lawsuit is subject to the right to record material fees. In the proceedings before the Metropolitan Court a legal representation is mandatory.

EXPLANATORY STATEMENT

I.

Facts, history

The Authority received a public interest announcement on 9 July 2019, which the Client is online called for a vulnerability in his system affecting personal data, including special data attention: the website operated by the Customer, the appointment book https://www.hungariamed.hu system - https://bejelentkezes.hungariamed.hu - treated medical findings and referrals publicly available or downloadable for unauthorized users.

Attached to the application was a screenshot taken by the applicant of from the interface that displays the list of documents stored in the appointment system. THE The applicant said that he had already reported the problem directly to the Customer, however no feedback was received and the error was not corrected.

On the basis of the public interest notification, the Authority will initiate an official inspection on 18 July 2019 decided to verify that the Client has fully complied with the general Data Protection Regulation 33-34. obligations set out in Article In the public interest announcement In order to clarify and supplement the information contained in NAIH / 2019/5606/3, then later in its orders NAIH / 2019/5606/5 called on the Client to make a statement, to which the on both occasions he replied on time. Based on the findings of the audit, the case is special data pursuant to Article 9 (1) of the General Data Protection Regulation (health data)

likely to be at high risk due to the

due to failure to comply with the notification obligation in accordance with Section 60 (1)

On 14 October 2019, the Authority adopted Articles 32 to 34 of the General Data Protection Regulation.

has initiated a data protection authority proceeding against the Customer for alleged violation of Articles

NAIH / 2019/5606/7 and further clarification of the facts

In order to do so, the Customer requested a further statement, to which the Customer replied within the prescribed time limit.

2

Information obtained following a public interest notification and official control and subsequently a

During the official procedure, on the basis of the Client's statements and data, the Authority shall

revealed the following.

THE

vulnerability

the

https://bejelentkezes.hungariamed.hu/doc/,

or

the

https://fogleu.hungariamed.hu/doc/ URLs where .pdf containing patient findings

documents were stored. The web server has the above special URLs ending in / doc /

instead of displaying the requested appointment book, all on the web server

content is listed on the screen. This allowed anyone, knowing the links above, to

without logging in, that is, without registering on the site, access the online interface

for documents containing personal data.

The Authority's IT security officer found that he was involved in the data protection incident

The vulnerability in this system may have occurred due to the fact that the Client is on its server

applied incorrect configuration settings. If the settings are correct, a / doc /

When you type a URL that ends in, the server displays an error message stating that the URL is

not found on server. However, due to this configuration error, the affected URLs
the server has displayed the directory structure on the web page, so it is stored there
documents containing personal data were accessible. (see case
NAIH / 2019/5606/2. information security expert opinion).
In the system affected by the data protection incident, the Customer has approximately 15,000 personal data
manages: the names and births of the employees of the partners in a contractual relationship with the Client
place and time, mother's name, TAJ number, e-mail address, telephone number, address, position, and
health data. The personal data of the data subjects in the appointment system for the first time
will be registered and, after the inspections, their findings will be uploaded, which a
the results of their laboratory, specialist and occupational health tests
including their family history.
In its response to the Authority, the Client stated that it existed on its website
only from the order received by the Authority on 19 July 2019. The
According to a customer, previously it was just a marketing, service-selling, rioting
received a letter with a tone that did not contain any content indicating a specific privacy incident. The
Based on this, the client performed a mini-audit of the IT systems used by him,
however, this did not identify an IT risk. Indicated in the order of the Authority
immediately launched an internal IT security audit to detect the vulnerability,
which on July 19, 2019 revealed a single vulnerability in its IT system. The
Customer has detected that the ID can be overwritten in the online query query URL,
and in this way documents may also be retrieved from the system.
During the examination by the Customer, the log files of the IT system were also analyzed.
The available files of these did not contain any data queries that were examined
would have actually referred to unauthorized access in the province, and the Customer would not have indicated otherwise
became aware of unauthorized access to the data.
In view of the existing vulnerability, a data protection incident has been identified

occurrence. During the risk analysis carried out in relation to the data protection incident, the

Customer has determined that it is not likely to pose a risk to the rights of those concerned and

3

given that unauthorized access to data is not

can be determined, or the error was corrected immediately after detection, so the incident

The Client did not consider it necessary to notify the Authority and inform the data subjects.

At the request of the Authority, the Client presented its current IT Security Policy (a

hereinafter referred to as "IBSZ"). According to this, “accountability and

a registration and logging system (security log) to ensure audibility

to be traced back to the 14 days preceding the reference period

major events in the IT system, in particular

which affect the security of the system - and thus the possibility of access rights

unauthorized access and, where possible, access

identification of the person. "

The IBSZ lists the minimum requirements for registration in the logging requirements

a list of events, including check-in and check-out. The Authority

in this regard, it found that any potential vulnerability arising from the identified vulnerability

accesses cannot be included in the logging scope of logins and logouts because it is affected

personal data for anyone without a link to the site without registration

were available. The Client is a public interest notifier as well as the Authority for IT Security

did not detect any inquiries made by his staff member during the official inspection

despite the fact that it took place within the logging time interval included in the IBSZ. The log files

as a result, they were not in a position to determine whether there was an unauthorized occurrence

access to the system.

Customer has not been able to determine exactly how long the vulnerability itself has existed since

system. However, after becoming aware of the incident, he perceived the deficiency

was immediately remedied. Not only the ID but also the login on the web server

user is also checked, so by rewriting the ID, only that user

it is possible to query your documents.

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

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

The data stored in the scheduled appointment system is a vulnerability unknown to the Customer

as a result, bypassing the system for unauthorized persons

have become available, however, no actual data access can be established. The client

considers that, in view of this, the incident is unlikely to pose a risk to those affected

fundamental rights and freedoms and therefore to the Authority

there is no obligation to inform those concerned about the incident.

In the course of the procedure, the Authority repeatedly tried to call on the notifier of the public interest to:

forward to the Authority the requests in which the vulnerability has been identified

Towards a customer. The notifier did not react to these until the end of the official procedure.

By order NAIH / 2020/952/2 of 6 March 2020, the Authority notified the Client that

carried out evidentiary proceedings in the case and informed that during the evidentiary proceedings

information security expert opinion - rules on access to documents

may be informed and may submit a motion for further evidence;

and called for a statement of revenue for 2019. The Client is required for the order

The Authority replied within the deadline and submitted a request for access to the file, which was granted by the Authority in

March 2020

On 12 December, by order No. NAIH / 2020/952/6, the Customer also approved

sent him a copy of the information security expert opinion.

at your request

the

According to the statement made by the Client in the reply letter dated 16 March 2020, the year 2019 is closed
and its balance sheet will be prepared in May 2020, following the audit, as follows
no clear revenue data is available for this. The current estimated revenue is 2019
HUF 800,000,000 in respect of which was determined by the Client on the basis of management's estimate. The client
it also informed the Authority that it was the result of an IT investigation carried out in the meantime
found that the privacy incident is believed to be about 9,000 personal
may have affected your data. The Customer has amended its incident record accordingly and repeatedly
sent it to the Authority.
Customer will become aware of the information security expert opinion on April 3, 2020
submitted a statement informing the Authority of the following. Customer a
unauthorized access was notified by the Authority, which was immediately and fully complied with
largely eliminated. Immediate elimination of data security risks and their
the following technical and organizational measures in order to eliminate them completely in the future
carried out. He took care of the / doc / directory on the web server immediately
after the blocking, it could no longer be unauthorized persons to the contents of that folder
accessed by. He conducted an external IT security audit, during which he verified it
the data retrieval functions of the systems used, the potential risks of data leakage
to prevent. The investigation revealed that access to the file
"Information Security Expert Opinion in Case NAIH / 2019/5656"
Apart from the vulnerability identified in the expert opinion on
vulnerabilities, unauthorized access, queries, information leaks
information.
The php-based codes of the appointment system have been redesigned by the Customer, the previous one
procedural approach has been redesigned to be object-oriented, providing even greater security
provides for data storage. Customer will use the encryption of the libraries, the authorization levels and the
also tightened user access, eliminating potential

system-independent data misuse. It also reviewed its development principles and policies,

as well as further information security training for development colleagues

in order to make any own system development only for information security requirements

with full effect.

II.

Applicable legal provisions

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

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

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

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

the general data protection regulation applies to data processing.

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

"security incident" means a breach of security which

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

loss, alteration, unauthorized disclosure or unauthorized disclosure

results in access.

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

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

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

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

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

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

without undue delay after becoming aware of the data protection incident

notifies the controller.

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.

Pursuant to Article 9 (1) of the General Data Protection Regulation, health data a

belonging to a special category of personal data and, as such, a higher level of protection

personal data requiring personal data (special personal data), subject to the provisions of Regulation (53)

subject to recital.

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

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 an adequate level of data security, including, inter alia, (in accordance with point (b))

the systems and services used to handle personal information are kept confidential

integrity, availability and resilience.

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.

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

(hereinafter: the Information Act) 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.

6

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 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. Articles 32 to 34 of the General Data Protection Regulation in the event of a breach of Article

the upper limit of the court that may be imposed is Article 83 (4) (a) of the General Data Protection Regulation

equivalent to EUR 10 000 000 (EUR).

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

disclosure of the identity of the processor, if the

This Decision affects a wide range of persons through the activities of a body performing public tasks

or the gravity of the infringement justifies disclosure.

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

III.

Decision

1. measures related to the handling of the data protection incident

According to the Client, the data protection incident is first reported to the Authority

NAIH / 2019/5606/3. an internal investigation following an order clarifying the facts of the case

on 19 July 2019. The public interest notifier, on the other hand,

that you have previously reported the vulnerability to Customer.

The Authority repeatedly tried to invite the public interest notifier to send it during the procedure

requests to the Client indicating the vulnerability, however, the notifier is the official

did not react until the procedure was completed. However, the fact of the infringement is due to the following

can also be determined on the basis of available data.

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.

The privacy incident was not reported before or despite the fact that a

Authority initiated its official inspection and then the present official proceedings against the Client. THE

the Client justified the non-notification on the basis of the risk analysis performed by the Client

the data protection incident is not likely to jeopardize the rights of the data subjects; and

freedoms.

The Authority considers that the risk assessment of the incident by the Client is not acceptable. The,

that the Customer does not have evidence that the IT

the vulnerability in its system has actually been exploited by unauthorized persons

would not be sufficient to establish that personal data are unauthorized

no access. The Authority found during the proceedings that the Customer is logging

system was not suitable for detecting external access as it was being examined by the Customer

IT Security Officer of the Authority and, in the past, the public interest notifier

accessed the processed data without the Customer noticing.

Nor can the Authority accept the Client's argument that the incident was not due to it

because the vulnerability was corrected immediately after it was detected. That

that is, exactly how long this vulnerability has existed in its IT system, the Customer

he was also unable to establish, so he was not able to establish, in the IBSZ

whether unauthorized access occurred outside the busy logging time slot.

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

data processing may result in identity theft or misuse of identity,

it is considered to be fundamentally risky. Name, date of birth, name of mother and

in particular, the number of TAJ data that can be used to identify identity,

identity theft.

Furthermore, the high risk classification of data subjects' rights is in itself justified by the fact that

that the Customer has a large number (approximately 15,000) stored in the system affected by the incident

personal data includes health data, which is covered by the general data protection regulation

According to Article 9 (1), they fall into a special category of personal data. These data

The exclusion from the general concept of personal data is justified by the fact that such information is

more sensitive aspects of the life of the person concerned and therefore unauthorized

The possibility of getting to know or making it public can also be particularly damaging

concerned. The unlawful processing of such data may adversely affect the reputation of the individual,

private and family life, may be the reason or justification for discrimination against the data subject

against. The aforementioned recital 75 deals with the processing of health data

in itself constitutes a processing operation which infringes the rights of the persons concerned and

fundamentally risky for his freedoms.

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 the Authority.

The Authority also considers that the incident is of a high risk which:

justifies that, pursuant to Article 34 (1) of the General Data Protection Regulation,

stakeholders.

The Authority also considers that information on the incident is explicitly required to

whereas the risk to the data subject's privacy is the use of personally identifiable information (name,

date of birth, place of birth, mother's name, TAJ number, address, e-mail address, telephone number)

in the event of its disclosure being of such a nature (may be committed in possession of this information

misuse of identity), the risks of which, as set out in recitals 85 (86) of the General Data Protection Regulation, can only be

mitigated

effectively if those concerned are aware of it and can do what they need

held further action. In addition, the involvement of health data is high risk

results in a privacy incident, as knowledge of these may provide a basis for impairment

discrimination, but may even affect the private and family life of the person concerned, which is why

it is also appropriate to inform those concerned.

The Authority draws attention to Article 34 (3) of the General Data Protection Regulation

(c) if the information would require a disproportionate effort, the persons concerned

shall be informed by means of publicly available information or a similar measure shall be taken,

which ensures similarly effective information to stakeholders.

2. Findings on data security measures

In order to assess the risk posed by the incident, the Authority also examined whether

Customer's compliance with data security directly related to the occurrence of the incident

requirements.

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

in order to guarantee a level of data security appropriate to the degree of risk,

implement technical and organizational measures appropriate to the state of the art, including

including the processing of personal data pursuant to Article 32 (1) (b) of the Regulation

ensuring the continued confidentiality and integrity of systems and services,

availability and resilience.

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.

With respect to access to the managed data, the Customer was unable to demonstrate that access to them

wondering how many people from outside had unauthorized access. According to his statement, his logging system is not

has demonstrated such access and the other tools it uses (hardware and

software firewalls, network security program). The Client during the procedure so

stated that all pdf downloads are logged (subject to registration and registration

but they cannot detect external access during the relevant period. In comparison, the

both the Authority's IT security officer and the public interest whistleblower had access to the data processed

from outside the period. The information security made by the Customer during the proof process

even after obtaining an expert opinion, the Authority did not receive any further information

which would have resolved this contradiction. The Customer also does not

has been able to determine how long the vulnerability has existed in its IT system.

Having just one simple web link to your managed health data

In addition to preventing unauthorized access, specific access (in this case

external document downloads), or the ability to log external malicious attacks,

and network security devices that can identify the unauthorized access person are adequate

In addition to the settings, the up-to-date application has also been defined in the Client's IBSZ as
internal rule. The Authority notes that in its view these internal rules would otherwise
in accordance with Article 32 of the General Data Protection Regulation,
According to the current state of technology, a large number of health measures can be expected
data management. This is especially true for market players who also benefit financially
with their main activity related to the processing of such data. The Customer is the unauthorized
insufficient disclosure of access is therefore not limited to its own internal rules,
nor did it meet the generally expected level of protection commensurate with the risks.
Due to the inability to detect external accesses and downloads, the Customer has violated the
Article 32 (1) (b) of the General Data Protection Regulation.
Health data - as defined in Article 9 (1) of the General Data Protection Regulation
special data - as such, as explained in the previous sections
results in high-risk data management. In handling such data, therefore, data controllers
is highly expected to have a high-risk technical and organizational balance
take measures to ensure data security.
This is confirmed by Article 32 (2) of the General Data Protection Regulation, which states that
in determining the appropriate level of security, the
risks arising from the processing of data, in particular those transmitted, stored or otherwise
accidental or unlawful destruction or loss of personal data
unauthorized disclosure or unauthorized disclosure
from access.
Given the vulnerability in the system affected by the data protection incident
due to the fact that the Customer did not process personal data
applied appropriate security settings to the data subject's system, which allowed
that anyone with knowledge of the link to the site can access it without registering on the site
for documents containing personal data stored on the online interface, - the Customer also

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

3. Sanction and justification applied

The Authority, in clarifying the facts, found that the Client had violated the general

Article 32 (1) (b), Article 33 (1) and

Article 34 (1). In view of this, the Authority instructed

the Customer to take the necessary measures to ensure that those concerned

Article 34 of the General Data Protection Regulation

according to

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 the Customer to pay a data protection fine

obliged.

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

Infringements committed by the Customer pursuant to Article 83 (4) (a) of the GDPR are

constitute an infringement of a lower fine.

The Authority considered the following as an aggravating circumstance:

-

The handling of personal data affected by the incident is higher due to the nature of the data

therefore, data controllers should exercise extreme caution

in order to guarantee a level of data security appropriate to the degree of risk, the Customer

nevertheless, a large number of personal data (approximately 15,000), including

the confidentiality of the system used to manage health data

has not taken appropriate measures to ensure The Customer is also

after becoming aware of the incident, - despite the data involved

the nature of the special personal data is obvious, - did not provide the Authority with

notification and information measures for those concerned, such as

his conduct is particularly blatant. [Article 83 (2) (a) GDPR].

-

The Authority found that a fundamentally high-risk, special data also

in order to prevent unauthorized access and

data security measures that are disproportionate to the risks

employed when accessing health and additional personal information is extremely easy

it could be accessed from the outside without the Customer noticing. Such data

safety preparedness to deal with, health activities are the main

profit-based businesses. [Article 83 GDPR

Paragraph 2 (d)].

-

The breach also affects special categories of personal data. For such data

in the event of an infringement, more severe sanctions may be justified because of their unauthorized knowledge

may have significant consequences for those concerned. [Article 83 (2) (g) GDPR

point].

-

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

No privacy incident has been reported by Customer, despite the fact that

Authority initiated its official inspection and then the present official procedure with the Client

against. [Article 83 (2) (h) GDPR].

The Authority considered the following as mitigating circumstances:

-

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

that the persons concerned have suffered damage as a result of the infringement [Article 83 (2) (a) GDPR point].

-

From the facts revealed, it can be concluded that the infringement was not intentional, that is to say Caused by customer negligence. This is also indicated by the fact that the Client is about the incident immediately after becoming aware of the vulnerability, the detected vulnerability was taken [Article 83 (2) (b) GDPR].

11

The Authority shall decide on the legal consequences of general data protection did not consider Article 83 (2) (c) (e) (f) (i) (j) and (k) of the Regulation to be relevant.

In view of the above, the Authority considers it necessary to impose a fine, only the Infotv. 75 / A. Did not consider it appropriate to apply the warning under

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

In imposing the fine, the Authority finally took into account that the Customer's 2018 according to his report, he had a revenue of HUF 631,480,000. According to the Client's statement, the year 2019 its closing and balance sheet will be prepared in May 2020, so this is not the case clear revenue data is available, based on management estimates, the Client's revenue in 2019 is 800 It was HUF 000,000. In view of the gravity of the infringement and the management data of the Client, the imposed the amount of the fine can therefore be considered proportionate in the Authority's view.

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. 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.

74/2020 on certain procedural measures in force during an emergency. (III. 31.)

According to Section 35 of the Government Decree (hereinafter: Government Decree), unless otherwise provided by this

Decree

the emergency does not affect the running of the time limits.

12

Pursuant to Section 41 (1) of the Government Decree, the court is hearing at the time of the emergency

acting outside. If the lawsuit were to be heard outside the time of the emergency, the plaintiff would then

may request the court to adjudicate the emergency instead of adjudicating

postpone until the end of

(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 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, April 27, 2020

Dr. Attila Péterfalvi

President

c. professor