Case number:

Antecedent:

NAIH / 2019/2668/2

NAIH / 2018/5457 / V

Subject: Ex officio

starting

data protection authority

closure of proceedings

SIX SECTIONS

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

Democratic Coalition (registered office: 1132 Budapest, Victor Hugo u. 11-15.) (Hereinafter: Client)

initiated on 21 November 2018 in connection with a data protection incident involving

in an official data protection procedure

(1) finds that:

(a) the Customer has not complied with its obligations under Article 33 of the General Data Protection Regulation

the obligation to report an incident,

(b) the Customer has not complied with its obligations under Article 34 of the General Data Protection Regulation

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

(a) inform the persons concerned of the fact and circumstances of the incident,

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

(b) record the fact of the data protection incident, its consequences and the action taken to remedy it

measures pursuant to Article 33 (5) of the General Data Protection Regulation

in the register,

3) due to the violation according to point 1), obliges the Client to make this decision final

within 30 days of becoming

HUF 11,000,000 data protection fine.

4) order the final decision by publishing the identification data of the data controller

disclosure.

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.

The fine is a HUF settlement account for the collection of centralized revenues of the Authority

(10032000-01040425-00000000) shall be paid for. When transferring the amount a

NAIH / 2019/2668 JUDGMENT. number should be referred to.

If the Customer fails to meet the obligation to pay the fine on time, a late payment surcharge

is obliged to pay. The amount of the late payment allowance is the statutory interest affected by the delay

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

In the event of non-payment of the obligations under point 2) or of the fine and penalty for late payment

the Authority shall order the enforcement of the decision.

There is no administrative remedy against this decision, but from the date of notification

within 30 days of the action brought before the Metropolitan Court in an administrative action

can be challenged. The application must be submitted to the Authority, electronically, which is the case

forward it to the court together with his documents. The request for a hearing must be indicated in the application. THE

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

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.

IND OKOLÁS

I. tényállás, elŐzmények

The Authority received a public notice on 23 August 2018 calling on the

Please note that it can be linked to the website http://web.dkp.hu operated by the Customer, personal

The user database containing the data is publicly available on the Internet at

https://defuse.ca/b/DIOCGRER7ZE1qVeDyVKpg1.1 Database user email

addresses, usernames, and passwords required to log in in encrypted form

contain. The database could have been made public by an unknown attacker who had one of these

reported in a blog post, 2 exploited the vulnerability on the website and then accessed it

uploaded to the said https://defuse.ca/b/DIOCGRER7ZE1qVeDyVKpg1 address.

On the basis of the public interest notification, the Authority initiated an official inspection on 14 September 2018

in order to verify that the Customer has fully complied with the general

Data Protection Regulation 33-34. and the information requirements set out in Article

CXII of 2011 on the right to self-determination and freedom of information Act (hereinafter:

Infotv.) In force, of which you have notified the Customer. The notice to the Customer is the return receipt

received it on 19 September 2018 on the basis of his testimony. The Authority NAIH / 2018/5457/3 / V., Then

later NAIH / 2018/5457/5 / V. and NAIH / 2018/5457/8 / V. clarification of the facts in his orders no

invited the Client to make a statement for the purpose of

answered. Based on the findings of the audit, Article 9 of the General Data Protection Regulation.

Special data according to Article 1 (1) (data on political opinion, party affiliation)

likely high risk due to its involvement and Article 33 (1) of the Regulation

due to failure to notify properly - Infotv. Section 60 (1)

the Authority initiated on 21 November 2018 a data protection authority proceeding concerning

You have notified a customer. In the course of the proceedings, in order to further clarify the facts, the Authority will: a

By order No. NAIH / 2018/5754/11 / V on another request and declaration of the Client

decided which order the Customer responded to within the prescribed time limit. It was later extended by the Authority

the subject of the data protection authority proceedings is governed by Articles 33-34 of the General Data Protection

Regulation. Articles

NAIH / 2019/2668 of 8 March 2019

notified him under case number.

1

The database was saved by the Authority and then named “DK database.xlsx” containing the database and

along with an authentication key generated from a file with the extension NAIH / 2018/5457/7 / V.

under registration number. A separate note was made on this.

2

A description of the methods described by the attacker is available at

https://h4x0rd0t.wordpress.com/2018/08/22/dkpwnelkurtuk-no-kitit-vagyon/. The attacker published the article on August 22,

2018. The Authority has the article on the matter

2018/5457/2 / V. as an annex to its file (information security expert opinion)

down and handles.

3

Information obtained following a public interest announcement and official control, followed by

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

revealed the following.

It is available on the website of the hacker who carried out the attack (in the blog post cited above)

based on the information, the attack is due to a database vulnerability resulting from the settings of the website

could have been realized, which consisted in the attacker's ability to communicate through the website

directly to the database so you could give it instructions.

The Customer claims the vulnerability through which the attacker was able to access the

caused by an error in one of the redirects affecting the website. The point of this mistake is

that the virtual hosting3 service also used by the Customer to operate the website (in short:

vhost) to redirect the dkp.hu (main) domain to the web.dkp.hu subdomain. Here is the

not in the server server redirect command at the time of the incident

it was properly regulated that other routes written behind the dkp.hu domain would also be redirected avoid. Requests for other routes written behind the (main) domain of dkp.hu - even manually

by default, they point to the vhost directory in all cases. The server is such another

when fulfilling requests, it took by default what was first in the list. THE

and first on the list were files from a 2013 test system with user data in it.

Therefore, if an attacker has entered a request for another route behind the (main) domain dkp.hu,

so, due to an incorrect setting, the published users were able to access it

for files that also contain a database.

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

system. Vhost configuration files on August 23, 2018 (after the Customer

self-acknowledged of the incident) were amended at 09:15 to read as follows:

so that the files can no longer be accessed from the outside. According to the Customer's statement, the error is in this

After repairing the system, he checked the system with the help of his experts, a further error of a kind that

which was also described in the hacker's blog post could no longer be after the fix

to generate.

Due to the vulnerability, an attacker could recover the

data of all users stored in the test system. The attacker also uses the command he uses

published by. Using the published command, he is low-skilled in terms of IT

it also allowed people to take advantage of this error and the database

to obtain.

The published database contains the full name of the registered users, the registration

username, e-mail address and - encrypted - required to log in

password.

The passwords on the database server were encrypted (encrypted) using an algorithm called MD5,

however, which encryption provides very poor protection as it can be decrypted in 1-1 minutes

password, even free websites and applications available to anyone on the Internet

using or even using a target program written for this purpose. IT security expert of the Authority in an attempt to decrypt some of the passwords disclosed by the hacker and

3

Using a virtual host (vhost for short) service enables a unique server machine to

to have a web server that can serve multiple domains.

4

From a database saved by an authority and without success. This was done by the Authority in 2018/5457/2 / V.

documented in IT Security Expert Opinion No.

The database contained a total of 11,614 records. Of these, there are lines where

not all of the data listed above were found, but are included in most of the rows

some data from these data types. The data also includes records that

from which the administrative user can be inferred.

According to the Client's statement, the published database is not on the web.dkp.hu website

data of currently registered users, but was made at the end of a previous year, 2013

contains test system data that, during the creation of an internal record system, test

created for this purpose. However, this registration system was never complete, so for good

remained in the test phase. However, this test database was randomly selected, legally

have been collected with data collected from real, natural persons and are not fictitious, fictitious,

contains randomly generated data.

The Client also informed the Authority that no test system was finally introduced

its purpose would have been to inform its users about and related to their membership in the party

would have provided information such as membership fee balances, payments, etc. THE

test system to maximize the number of user accounts for testing

data used in the lawful collection of signatures (typically in 2012)

were randomly selected from the contact information obtained.

At the request of the Authority, the Client also performed in the published database one

inspection. Based on this, it narrowed the data and removed the rows from the table that where email was empty / accented / dotted / duplicated

(i.e. it was listed twice in the database). You have also removed the lines where the name field is empty

volt. Based on these, a total of 6,987 affected personal data are included in the database.

At the request of the Authority, the Client has also indicated in the table which persons are

at any time in the past or present in the party

- have held any office,

- party members of parliament,

- municipal representatives of the party,

ran as a candidate in parliamentary or municipal elections, or

- for any other reason, their name is in the public interest because of their relationship with the party.

In accordance with the above criteria, a total of 505 cases were classified by the Client as

the names of the persons in the database are made public in the public interest.

The test system database can be divided into three categories based on the source of the data

to share stakeholders:

- members,

- registered sponsors,

- sympathizers.

There are two ways to record people in the member and registered sponsor database:

via the Internet or on paper. In the first case, on the registacio.dkp.hu website, the given

the person concerned shall complete the requested information and declare that he or she will continue to be a member or as

a member

registered supporter wants to join the party. The person completing the registration will thus become a member,

or a registered sponsor candidate. After that, the online registration after sending the IT

the system automatically classifies the person concerned, so they go to the constituency president by address

the application for registration of that person. It is then presented by the constituency president at a general meeting the admission of the new member. Finally, the constituency president indicates to the data controller group the new member who will record him in the database.

On a paper basis, some individuals were registered as members or supporters in such a way that

or the registered sponsor-candidate on a paper-based, sealed envelope.

application form for the party. The data management team then processes the data provided and

records the registration application. The application is automatically classified after the IT system

to the constituency president by address. The application is then processed in the same way

happens like the web interface.

In both cases, you will receive a welcome email after the registration process is complete.

In this e-mail you can find the system required to access the interface on www.dkp.hu.

username automatically generated by. The password required to log in is the member / registered

support after the first login. Sympathizers cannot access the website online

surface.

According to the Client, they entered the sympathy database in the following three ways

recorded persons:

-

At alairas.dkp.hu, one of the signature collections is available online

signature with data,

paper-based signature collection sheet by entering and signing data into data management

by consent, and

in Robocall, during a telephone survey, the appropriate push button is provided by that person

by pressing.

Once the data has been provided voluntarily, only the data management team can record sympathizers

to the database.

The test database thus the party using the above method, from members, registered sponsors and

data collected from sympathizers were included on a trial basis. Not all of them, but randomly selected some of them. Since the system was never armed, the test users have never had access to the system.

The incident (the possibility of unauthorized access to the data) is specific date unknown. According to the incident blog post, the detection of the vulnerability is a by a hacker running a blog as early as April 2018, and it was already notified by Customer. However, there are no other options available in this regard than the blog post clear and credible evidence. The Customer has stated that the incident is the first received an alert by e-mail on the evening of August 22, 2018, informing him of the attack fact. The sender of the message was not otherwise named by the Customer. Customer is aware of the incident did not inform those concerned. He stated that the data concerned were out of date, obsolete, so the data of the current sympathizers and members of the party stored and managed by the party he said he was not affected by the incident. The Customer did not take the incident for the same reason registered pursuant to Article 33 (5) of the General Data Protection Regulation, claiming that that the case did not affect his live database.

II. Alkalmazott jogszabályi rendelkezések

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. The general privacy policy Pursuant to Article 99 (2) of the Regulation, the Regulation shall apply from 25 May 2018.

According to Article 4 (12) of the General Data Protection Regulation, "data protection incident" means security damage to personal data transmitted, stored or otherwise handled accidentally or unlawful destruction, loss, alteration, unauthorized disclosure or resulting in unauthorized 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. […]. The general

Article 33 (5) of the Data Protection Regulation requires the controller to keep records of

data protection incidents, indicating the facts related to the data protection incident, its

effects and remedial action taken in a manner that allows for monitoring

authority to verify compliance with the requirements of Article 33.

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.

Subject to Article 9 (1) of the General Data Protection Regulation

personal data belong to a special category of personal data and, as such, are higher

personal data requiring a high level of protection (special personal data), subject to the provisions of Regulation (53)

subject to recital.

Infotv. Pursuant to Section 2 (2), the general data protection decree is indicated therein

shall apply with the additions provided for in

Infotv. Enforcement of the right to the protection of personal data pursuant to Section 60 (1)

In order to do so, the Authority may initiate ex officio data protection proceedings. The data protection authority

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

Ákr.) Shall apply with the additions specified in the Information Act and the general

with derogations under the Data Protection Regulation.

The Ákr. Pursuant to Section 103 (1), the Ákr. Initiated ex officio proceedings upon request

provisions of the Act on With the exceptions set out in §§ 103 and 104

apply.

Infotv. Pursuant to Section 61 (1) (a), it was taken in a data protection official proceeding

In its decision, the Authority Data management specified in Section 2 (2)

defined in the General Data Protection Regulation in the context of

may apply legal consequences. Article 58 (2) (b) of the General Data Protection Regulation

The supervisory authority shall condemn the controller or the processor if

data processing activities have infringed the provisions of this Regulation or the same paragraph (d).

instructing the controller, acting in accordance with

that its data processing operations are carried out, where appropriate in a specified manner and within a specified period of

time;

bring it into line with the provisions of this Regulation.

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 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

the maximum fine that may be imposed is EUR 10 000 000 (EUR).

Infotv. 75 / A. § according to Article 83 (2) - (6) of the General Data Protection Regulation

exercise the powers set out in paragraph 1 in accordance with the principle of proportionality,

in particular by the legislation on the processing of personal data or the European

Infringement for the first time of the requirements laid down in a binding act of the Union

in accordance with Article 58 of the General Data Protection Regulation.

primarily by alerting the controller or processor.

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

III. Dönt és

a) Failure to report a data protection incident

The Customer became aware of the data protection incident no later than the evening of August 22, 2018. The

The incident has not been reported to date despite being initiated by the Authority

official control and then the present official proceedings against the Client.

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 Customer's justification for failing to notify is that

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

viewed, does not stand still. The fact that the database may be old, outdated data

contained that there would have been only one so - called test database, and that the Customer had

did not affect its current, live databases, there was no access to them, no

acceptable.

It is irrelevant to the assessment of the risk to the parties involved in the case that

when the data was generated and for what purpose and as part of what system the Customer used it

originally collected. The data controller is responsible for the processing of personal data processed by him

requirements throughout the data processing period. And that is the given

In the case of data subjects involved in an incident, the

personal information may no longer be current, it does not in itself mean that it is even personal

would have lost the character of the data, even special data.

In particular, this customer reference is not relevant

regarding the disclosure of data (name, e-mail address, username, password),

for which the risk to the data subject's privacy is typically high. These data misuse of identity is easy.

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

that the incident involved personal data from which the data subject had a political opinion

a conclusion can be drawn. The significance of the risk to the data subject is not relevant

that this conclusion is not the most accurate on the basis of the database,

most relevant, as belonging to a political organization, even if it is a thing of the past,

in any case, it reflects the political opinion of that person. Plus from the database - no

regardless of the deficiency discussed below - in no way does the data reveal any

current or unrealistic nature - in fact, the data confirmed by the Customer's statement is true

were real data of persons. Finally, the argument in favor of a high risk rating is that these

specific data for most of the data subjects could not be ascertained from other sources, they

have been disclosed solely in connection with the present incident.

The data on the political opinion are Article 9 (1) of the General Data Protection Regulation

fall into a special category of personal data. Highlighting this data is a

the general concept of personal data justifies the fact that such information is relevant

they relate to more sensitive aspects of their lives and are therefore unauthorized to be disclosed

may be particularly prejudicial to the person concerned. This data is illegal

treatment can negatively affect an individual’s reputation, private and family life, is detrimental

may be a reason or justification for discrimination against the data subject.

Based on the Customer's statements, it is personal in the system affected by the data protection incident

data came from party members, registered supporters, and sympathizers.

Sympathizers at signatures related to political expression or by telephone

could be entered into the database through queries. Enter the data in each case

was voluntary, the data management was specifically related to the political activities of the party a

by collecting a sympathy database. The sympathizers could not enter the party www.dkp.hu.

in which case the Customer did not handle usernames and passwords.

The data of the members and registered supporters of the party were collected on the Internet or on paper Customer, and before entering the database, it had to be approved by the party in all cases competent constituency president. The data required for registration was then added to be sent by e-mail to the data subject, who was later able to create a website on www.dkp.hu a username and password pair required to log in.

Personal data collected in the manner and for the above purposes was later entered into the test database, which the data protection incident is involved. Data disclosed by the hacker for political opinion as the persons concerned can be clearly contacted with the activities of the party, they were sympathizers, supporters, and members of the party. To the database admission is part of a more complex registration and selection process in which the The customer has a direct influence on which persons can be included in the operations he or she operates database. Political is important when entering personal information processed in the database opinion, the existence of party preference on the part of the person concerned. These data are therefore without exception special personal data.

Recital (75) of the General Data Protection Regulation also confirms that if personal data which refer to a political opinion are processed, it shall be is fundamentally risky.

Finally, the incident is also considered to be high risk because, as described below, due to outdated encryption methods used in the database, belonging to users, and quite common among the average user is not necessarily different (mostly online, but even offline) username password pairs may have become known.

In view of this, the Customer should have reported the incident within 72 hours of becoming aware of it report to the Authority. By failing to comply with that obligation, it infringed the general rule Article 33 (1) of the Data Protection Regulation.

(b) Obligation to inform data subjects and record of the incident

In addition to the above, the Authority considers that the incident is of such a high risk

justification under Article 34 (1) of the General Data Protection Regulation

inform those concerned.

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,

e-mail address, username, password) is of such a nature (these data

misuse of identity), the risks of which

can be effectively mitigated if those concerned are aware of it and can do so

additional measures deemed necessary. In addition, it concerns political opinion

the involvement of personal data also typically results in a high-risk data protection incident,

whereas knowledge of these may give rise to discrimination, but even to the person concerned

it can also affect your private and family life, 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.

Finally, the Authority notes that under Article 33 (5) of the General Data Protection Regulation

data controllers must keep a record of all data protection incidents, regardless of their risk classification

to keep. It must indicate the facts related to the data protection incident and its effects

and the measures taken to remedy it. The Customer thus did not lawfully claim that

did not register the incident because it affected outdated data and therefore did not consider it

risky.

(c) Findings on data security measures

Incident management, reporting and related incident risk

Based on the findings of the investigation, the Authority also examined whether the Client

the extent to which it has complied with data security requirements. In this context, however, it is primarily data security requirements directly related to the management of the incident

examined to assess the risk posed by the incident.

However, the subject of the proceedings was not the subject of Article 32 of the General Data Protection Regulation (Art

security of data processing), however, the incident

due to its risk classification and the examination of the justification for the reporting obligation

it was absolutely necessary to address these issues as well. In the present case, it is the incident

risk assessment is inextricably linked to certain data security issues.

In this regard, the Authority's position is generally from a data security perspective

a risk mitigating factor may be that the data are out of date and no longer available

access to any living system operated by the controller, in particular if

the data controller used appropriate encryption in relation to them, but this is not the case here

state.

In the present case, the passwords were encrypted using an outdated technology

which, according to the state of the art, are now readily available free of charge

also anyone can decipher it. Article 32 (1) of the General Data Protection Regulation

on the basis of the data controller in the state of science and technology appropriate technical and organizational

measures must be implemented to ensure data security commensurate with the degree of risk

to guarantee. This includes personal data under Article 32 (1) (a) of the Regulation

proper encryption of data. If the encryption used is special expertise, time

and without cost, it becomes decipherable by anyone, so it is no longer appropriate for science

and the state of the art. The obsolescence of the applied technology makes sense

associated with an increased risk to encrypted data. This is also the case for an incident

in any case a risk factor.

It should be a high-risk condition for users in almost all cases

assessed in the opinion of the Authority if the purpose of entering a system is not properly or obsolete encrypted username and password pairs are disclosed. Of this

main reason that users use the same data may be different (mostly online, but even

offline) can still be used to this day. Users typically

do not generate a separate username and password for each Internet service,

but very often the same (or certain versions) are used.

The measures taken by the Customer to ensure data security are the technology used

therefore the risk of the incident to the rights and freedoms of those concerned

also increased.

Furthermore, it was clear from the decrypted passwords that it was not for that server

was an algorithm for validating password complexity. The Authority's IT security officer found one

user whose decrypted password was all lowercase.[4] For security reasons,

Authority does not consider it a good practice if the passwords of the users are not one in advance

according to a set of rules setting higher security requirements

they have to figure out what the system forces when entering the password (eg password

mandatory length, mandatory special characters, etc.). The reason is no

With a strong password validation system, users typically get as simple and

shorter passwords will be used. However, simpler passwords are easier for one to know

an external attacker to decipher or infer. In this respect, the Authority notes that

[4] See 2018/5457/2 / V. established in the file (information security expert opinion).

if this is not a password generation and strong password enforcement practice in the Client’s organization

within other IT systems, review it as soon as possible

justified.

(d) Sanction and justification applied

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

Article 33 (1) and (5) and Article 34 (1) of the Data Protection Regulation. THE

In view of the above, the Authority instructed the Client to

to record the data protection incident in the internal register and the data subjects

to inform.

The Authority examined of its own motion Article 58 (2) (i) of the General Data Protection Regulation

the need to impose a data protection fine in the light of Article 83 of the Regulation.

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.

As to whether the imposition of a data protection court is justified, the Authority is the general one

considered all the circumstances of the case under Article 83 (2) of the Data Protection Regulation. THE

Authority deems it necessary to impose a fine because the Customer has not complied with that

incident reporting obligation, including high-risk special data

in the context of the incident and did not inform those concerned, essentially in full

failed to perform his duties under the relevant legal requirements. Regarding to this

the Authority only the Infotv. 75 / A. Did not consider the application of the warning pursuant to §

appropriate.

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

determined.

The Authority took into account Article 83 of the General Data Protection Regulation when imposing the fine

(2) and the nature of the breach (by dealing with a data protection incident

failure to fulfill an obligation).

The Authority took the following factors into account when imposing the fine.

Aggravating circumstances:

-

-

-

The data protection incident involved a particularly high risk: a political opinion

concerned a large number of data subjects

the risk of further incidents for them, which also allows for the individual identification of data subjects

carrier data became available.

The Client was aware of the incident, the data involved is special personal data

is obvious, but did not do so to the Authority with the notification and the

information measures, so that its behavior is particularly high

degree to blame.

Outdated encryption technology affects the rights and freedoms of those involved in the incident

explicitly increased its risk to

The number of people affected by the incident is relatively high (more than 6,000 in total).

Mitigating circumstances:

-

Measures taken by the data controller to mitigate the risk: The Client is aware of the incident

immediately after becoming aware of it, took action on the cause of the incident

in order to eliminate.

The Authority is aware of the fact that during the procedure the Client invites the Authority to provide information

provided that the Client's conduct in this area was not

went beyond complying with its legal obligations - not as an attenuating circumstance in itself

evaluated.

In imposing the fine, the Authority finally took into account that the Customer had a 2017 year

according to his report, he had a revenue of 269,361,000 HUF. According to the Client's 2018 budget

It forecasted HUF 415,000,000 in revenue. The gravity of the infringement and the management data of the Client

The Authority therefore considers that the amount of the fine is proportionate.

ARC. Egyébkérdések

Infotv. Pursuant to Section 38 (2) and (2a), the Authority is responsible for the protection of personal data,

and the right of access to data in the public interest and in the public interest

monitoring and facilitating the enforcement of The general data protection regulation of the supervisory

the tasks and powers established for the authority under the jurisdiction of Hungary

as defined in the General Data Protection Regulation and the Information Act

according to the Authority. The competence of the Authority extends to the entire territory of the country.

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

there is an administrative remedy against him.

***

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

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

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

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

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

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

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

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

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

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

hereinafter: E-Administration Act), the customer is legal

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.

If the Applicant does not duly prove the fulfillment of the required obligation, the Authority shall:

it considers that it has failed to fulfill its obligations within the prescribed period. The Ákr. According to § 132, if a

the obligor has not complied with the obligation contained in the final decision of the authority, it shall be enforceable.

The decision of the Authority Pursuant to Section 82 (1), the communication becomes final. The Ákr.

The Ákr. Section 133 of the Enforcement - unless otherwise provided by law or government decree

ordered by the decision-making authority. The Ákr. Under section 134 of the enforcement - if

a law, government decree, or local government decree in a municipal authority matter

unless otherwise provided - by the state tax authority. Infotv. Section 60 (7)

to carry out a specific act contained in a decision of the Authority

the decision as to the obligation to conduct, tolerate or stop

shall be carried out by the Authority.

Budapest, March 21, 2019

Dr. Attila Péterfalvi

President

c. professor