NAIH-1855-4/2022

NAIH-8855/2021

Case number:

Antecedent:

Subject: decision

ex officio

data protection

in procedure

starter

official

H A T A R O Z A T

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

Kétfarkú Kutya Párt (headquarters: 1071 Budapest, Damjanich utca 26/b 3/1.) (hereinafter:

Customer) 2021.

on June 26 electronically 2A4E89072FB4FDC9D79327FA37F01AD

in connection with the notification of a data protection incident made on identification number July 14, 2021.

on December 2, 2021 due to the circumstances revealed during the official inspection initiated on

in official data protection proceedings initiated ex officio

1) establishes that

a) The customer has violated the handling of the personal data of natural persons

regarding its protection and the free flow of such data, as well as a

Regulation (EU) 2016/679 on the repeal of Directive 95/46/EC (the

hereinafter: General Data Protection Regulation) Article 32(1) and its a)-b)

points,

(2) when he did not apply a

data security commensurate with the risks of storing the data of party sympathizers and activists

measures.

also this article

b) Customer has violated Article 5 (2) of the General Data Protection Regulation, as a

Despite repeated calls from the authorities, he did not fully confirm what it was like

has taken measures to reduce the risks of a data protection incident.

2) Instructs the Customer to

a) with regard to Article 5 (2) of the General Data Protection Regulation, he certifies that a

To the authority that the data protection incident information of the affected parties is

in accordance with Article 34 of the General Data Protection Regulation, when, in what form and

he did it with content.

b) inform the Authority about how the data involved in the incident is managed

transformed in order to ensure data security commensurate with the risks

apply measures.

3) Due to the above violation, the Customer shall, on the 30th from the date of this decision becoming final,

within days

3,000,000 HUF, i.e. three million forints

obligates you to pay a data protection fine;

…… 1055 Budapest Tel.: +36 1

391-1400 ugyfelszolgalat@naih.hu Falk Miksa utca 9-11 Fax: +36 1 391-1410 www.naih.hu 4) Orders the final decision to be

published by publishing the Customer's identification data

disclosure.

The fine according to point 3) above is settled by the Authority for the collection of centralized revenues

HUF account (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 a

NAIH-1855/2022 FEES. number must be referred to.

If the Customer does not fulfill his obligation to pay the fine within the deadline, he is in default
must pay an allowance. The amount of the late fee is the legal interest, which is due to the delay
is the same as the central bank base rate valid on the first day of the relevant calendar semester. The delay
allowance is the forint account for the collection of centralized revenues of the Authority (10032000-
01040425-00000000 Centralized direct debit account) must be paid.
Non-fulfilment of the instruction according to point 2) and the fine and late fee according to point 3)
in case of non-payment, the Authority orders the execution of the decision, the fine and the late fee.
There is no place for administrative appeals against this decision, but it is subject to notification
Within 30 days with a letter of claim addressed to the Capital Court in a public administrative case
can be attacked. The letter of claim must be submitted electronically to the Authority in charge of the case
forwards it to the court together with its documents. The request to hold the hearing must be indicated in the statement of claim
must For those who do not receive a full personal tax exemption, the administrative court fee is 30
HUF 000, the lawsuit is subject to the right to record the levy. In the proceedings before the Metropolitan Court, the legal
representation is mandatory.
I N D O C O L A S
History and clarification of the facts
I.
1) On June 26, 2021, the Customer electronically 2A4E89072FB4FDC9D79327FA37F01AD
filed an incident report with the Authority for data protection concerning its data management on the identification number
regarding an incident he became aware of that day.
In the incident report, the Customer communicated the following to the Authority:
On June 26, 2021, the customer was informed that a total of six Excel files with the extension .xlsx -
which were previously managed by the Customer - directly, accessible to anyone
made available via the link https://ufile.io/f/wn8iy. The link is https://kuruc.info/r/2/23220
article available via The files were:
- Rósáné2 leaflet sending.xlsx

- PARTY MEMBERS.xlsx

- Country distribution.xlsx

- MKKP campaign applicants 2018 (Responses).xlsx

- MKKP Procurement Department.xlsx

-

at kimici (MKKP employees, subject areas).xlsx

2

tables patron

Based on the customer's report a

list of their members and operational data

also include contact information (phone numbers, e-mail addresses,

residential addresses, identity card numbers). Based on the Customer's report in the data protection incident

approx. The personal data of 2,000 stakeholders were affected, including applicants for the 2018 election campaign

data, the exact data of the party's supporting members, the names of the party's internal coordinators and assistants, a

the list of the party's 2022 election candidates. The customer did not know clearly at the time of notification

determine whether the data leakage is an external act (e.g. hacker attack) or internal

result of leakage. After the incident, access to view the files is restricted to the

it was withdrawn from all but the co-chairs.

The customer did not inform the affected parties about the data protection incident at the time of notification, but the

plans in the future, as he deemed it "significant" in terms of risks. Information is planned

set the date as June 26, 2021.

2) On July 14, 2021, the Authority launched an official inspection of the incident report

for the purpose of assessing whether the Customer fully complied with the handling of the reported incident

to the provisions contained in the General Data Protection Regulation. The Authority NAIH-5885-2/2021.

sent an order clarifying the facts to the Customer on July 14, 2021 and its framework

asked him to provide data between The Customer responded to the order within the deadline.

According to the customer, the tables were protected by restricting access, they are Google Sheets
managed online as a table. Previously, access to the tables was granted to the party leader
for its officials and activists using a link. Disclosure of tables
after that, access was restricted to senior party officials. They used to be insured for that
access to the activists as well, since according to the party's internal principles they can hold it directly
the relationship with each other.
In connection with the analysis of the file access log, the Customer could not determine that
whether they were accessed by an unauthorized external attacker, or whether the disclosure of the files was internal
result of leakage.
As the legal basis for processing the data, the Customer is Article 9 (2) of the General Data Protection Regulation
point d) of paragraph The data is collected directly from the activists
collected between 2017-2018. The purpose of collecting and further processing the data is party political
in its activities with political activity given by activists participating of their own free will
there was contact in the context.
In addition to the above, the customer contacted the file-sharing site called ufile.io, which stores files, and e-
they requested the removal of the files by e-mail as well as by phone. Customer to the kuruc.info website
he did not live by solicitation. By the way, the files were only within 48 hours of posting
are publicly available and free to download. The customer finally stated that, as far as he knew, there were none
data of public interest or of public interest among personal data that has been made public.
3) The Authority is acting
also referred to
Website available via the link https://kuruc.info/r/2/230220. Available through the website
a press release relating to the activities of the reporting party. Referenced in the article
https://ufile.io/f/wn8iy
another web page will open from where it is
was verified in the report

via a link

by its member

too

3

Excel files with the .xlsx extension also referred to in the incident report could be downloaded directly.

About the image and source code of the article and the website containing the files in .html format

backup, screenshots were also taken, and the databases were saved

in original .xlsx format. About saving the website and the files listed above separately in .sha

extension authentication files were created. These processes are regulated by Authority NAIH-5885-2/2021. no

documented in his memo.

The following personal data are included in the published tables:

a) Rósáné2 in the flyer sending.xlsx file:

Nature and description of personal data

Number of people affected

The following personal data of members: transferor

person's name, recipient's name, city

name, where the leaflet would be distributed,

name of city where the leaflets

will be collected, address where the flyers will be collected,

the person receiving the flyers is on the phone

availability

b) PARTY MEMBERS.xlsx file:

48

Nature and description of personal data

Number of people affected

on the "supporter member list" tab

Registration number of supporting members, complete

name, national individual constituency, address,

identity card number, phone number,

decision number and date, card number,

date of application, date of membership, withdrawal

fact, remark

"2022" tab

Registration number of supporting members, complete

name, national individual constituency, address,

ID card number, phone number, e-

e-mail address, date of membership, whether the

phone number, willingness to be active and

location, activity description, comment

509

476

4

35

60

20

495

12

52

27

On the "Member fee" tab

membership number, full name, application date,

date of decision, from when you have to pay,

from when you paid

On the "Wrongly notified members" tab

serial number, full name, telephone, e-mail address,

entry date, decision date, from when

you have to pay

"if he was a passivist, he would go here" tab

serial number, full name, national individual

constituency, address, identity card

number, telephone number, e-mail address, date

on the "card numbers" tab

card number, full name, number of orders

on the "to do" tab

full name, e-mail address, telephone number

on the "envelope" tab

full name, address, in some cases notification

title

On the "Sheet7" tab

full name, national individual constituency,

address, identity card number, e-mail address,

phone number,

c) Country distribution.xlsx file:

Nature and description of personal data

Number of people affected

"OEVK with map" tab

name of candidate, name of helper, name of coordinator, e-

email address, phone number, Facebook profile link

On the "Divided by country" tab

admin name, county coordinator name,

name of election coordinator

On the "Sheet7" tab

candidate name

117

56

57

d) MKKP campaign applicants 2018 (Responses).xlsx file:

Nature and description of personal data

Number of people affected

name, e-mail address, phone number, "where

would you campaign", "what can you help with?", "other

417

help"

e) MKKP Procurement Department.xlsx file:

In the table, asset purchases are entered, with the name of the project manager, in a total of 6 cases

by entering an e-mail address and telephone number.

f) in kimici (MKKP employees tasks, responsibilities).xlsx file:

The file lists the tasks of the party's 17 members (marked only by nicknames in several places).

included. The file also contains the Country distribution.xlsx table and the data in it

also on a separate ear.

4) After that, the Authority NAIH-5885-5/2021. for new data provision by order with file number

summoned the Customer by post on August 31, 2021, which was confirmed by the return receipt

according to the Customer's representative at its registered office on September 20, 2021. By the Authority

despite the set ten-day response deadline, no response to the order has been received to date.

Due to the lack of response, the Authority repeatedly invited the Client to make a statement NAIH-5885-

6/2021. with order no. on October 25, 2021. This order is sent to the Authority's Customer representative -

6

in view of the answer previously received from the Customer - delivered electronically, which was delivered by a

received on November 3, 2021 based on download confirmation. Five days prescribed by the Authority

despite the response deadline, no response to the order has been received to date.

5) Repeated failure to respond, further clarification of the facts and the general in the case

further alleged violation by the Customer of the obligations contained in the data protection decree

on the right to informational self-determination and freedom of information due to its necessary investigation

CXII of 2011 Act (hereinafter: Infotv.) with regard to Section 60 (1), the Authority 2021.

on December 2, decided to initiate official data protection proceedings.

On the initiation of the official data protection procedure, the Authority notified the Client NAIH-8855-1/2021.

the defaulter notified him by order with file number, and requested additional data from him

with regard to answers and further clarification of the circumstances of data management. Customer representative

received the order electronically based on the download certificate on December 6, 2021, and on

to this day he has also not responded.

In view of the above, the Authority NAIH-1855-1/2022. on January 27, 2022, with order no

due to non-response for the third time, a procedural fine of HUF 350,000 was imposed on the Customer by the

CL of 2016 on general administrative regulations. Act (hereinafter: Act) § 77

based on the fact that the lack of answers necessary to reveal the facts significantly hinders the

Authority's activities, thus the full disclosure of the facts in the case. The Authority also

He called on the client to immediately comply with the provisions of the previous order.

The customer downloads the order imposing the procedural fine and the repeated notice through his office portal

based on a certificate, he received it on January 28, 2021, but still did not respond to it, the procedural

did not pay the fine or take legal action against it within the stipulated 30-day deadline

not too much. The Authority also sends the order imposing the procedural fine by registered mail
sent it to the Customer's address, but the shipment was returned with a "not searched for" mark
on February 18, 2022.

II.

Based on Article 2 (1) of the General Data Protection Regulation, affected by the data protection incident
the general data protection regulation shall be applied to data management.

Article 4, point 12 of the General Data Protection Regulation defines what constitutes data protection
incident, based on this, "data protection incident": a security breach that affects the transmitted,
accidental or unlawful destruction of stored or otherwise managed personal data,
loss, alteration,
unauthorized
results in access.

According to Article 9 (1) of the General Data Protection Regulation, racial or ethnic origin,
referring to political opinion, religious or worldview beliefs or trade union membership
personal data, as well as genetic data, unique identification of natural persons
targeting biometric data, health data and sexual life of natural persons
or sexual orientation is prohibited.
unauthorized disclosure or for those
Applicable legal provisions

Article 5 (2) of the General Data Protection Regulation defines "accountability
principle", according to which the data controller is responsible, contained in Article 5 (1) of the regulation
for compliance with its principles and must be able to demonstrate this compliance.

Pursuant to Article 32 (1) of the General Data Protection Regulation, the data controller and
data processor the state of science and technology and the costs of implementation, as well as that
nature, scope, circumstances and purposes of data management, as well as the rights of natural persons and

taking into account the risks of variable probability and severity reported to his freedoms

implements appropriate technical and organizational measures to ensure that the risk

guarantees the appropriate level of data security. The decree includes, among other things, Article 32.

on the basis of Article (1) point b), the systems used to manage personal data and

ensuring the continuous confidentiality of services.

According to Article 32 (2) of the General Data Protection Regulation, security is adequate

when determining the level of

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

accidental or illegal destruction, loss, alteration, unauthorized

result from its disclosure or unauthorized access to them.

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

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

a data protection incident has come to his attention, he is notified by the competent supervisory authority based on Article 55

authority, unless the data protection incident probably does not entail a risk a

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

within an hour, the reasons justifying the delay must also be attached.

According to paragraphs (1)-(2) of Article 34 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

view, the data controller informs the data subject without undue delay of the data protection

incident. It must be clearly and clearly explained in the information given to the person concerned

the nature of the data protection incident, and at least Article 33(3)(b), (c) and (d) must be disclosed

information and measures mentioned in

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

(hereinafter: Infotv.) According to Section 2 (2) of the general data protection decree there

shall be applied with the additions contained in the specified provisions.

The Akr. On the basis of § 99, the authority - within the framework of its powers - checks the legislation

compliance with the provisions contained, as well as the fulfillment of the provisions of the enforceable decision.

The Akr. Based on point a) of paragraph (1) of § 101, if the authority finds a violation during the official inspection

experiences, initiates the official procedure. Infotv. Section 38 (3) and Section 60 (1).

based on Infotv. personal data within the scope of duties according to § 38, subsections (2) and (2a).

in order to enforce the right to data protection, it conducts official data protection proceedings ex officio.

8

his activity violated the provisions of the decree,

Infotv. Based on point a) of section 61 (1), the Authority in sections (2) and (4) of section 2

in connection with specific data management operations in the general data protection regulation

may apply specific legal consequences.

Based on points b) and i) of Article 58 (2) of the General Data Protection Regulation, the supervisory

authority, acting in its corrective powers, condemns the data manager or data processor if

data management

and Article 83

appropriately imposes an administrative fine, depending on the circumstances of the given case, e

in addition to or instead of the measures mentioned in paragraph

According to Article 83(5)(e) of the General Data Protection Regulation, Article 58(1)

in the case of non-compliance with the provisions on provision of access

up to EUR 20,000,000 or, in the case of businesses, the entire previous financial year

an administrative fine of up to 4% of its annual world market turnover can be imposed,

with the higher of the two amounts being imposed.

In addition to the decision, the Ákr. Sections 80 and 81 shall apply.

III. Decision

1. Findings related to the security of data management

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

and the state of technology and implementation costs, as well as the nature and scope of data management,

its circumstances and purposes, as well as the rights and freedoms of natural persons,

appropriate technical and

implements organizational measures to ensure that the level of risk is appropriate

guarantees level data security. The regulation includes, among other things, Article 32 (1) b)

point, the systems and services used to manage personal data are continuous

ensuring its confidentiality.

According to Article 32 (2) of the General Data Protection Regulation, security is adequate

when determining the level of

risks, which are especially transmitted personal data to unauthorized public

they result from making or unauthorized access to them.

According to the Authority's opinion, the data processing affected by the incident, i.e. the members of the political party,

personal data of sympathizers and activists (e.g. identification data, contact details, with party

related activities) is considered high risk. This is because it is common

Recital (75) of the Data Protection Regulation refers to data management during which political

data that can be associated with an opinion is treated as fundamentally risky. With this

in this context, it also considers it risky if data management results in discrimination

may arise, and also if the data management covers a large number of stakeholders. Finally, such data

management, of which identity theft or identity abuse (such

in this case, the identification data in the tables, such as: name, address, telephone number, e-mail

address, identity card number, Facebook profile link) may also be risky

considered by these provisions of the decree.

According to the Authority's opinion, a total of six items in the published table

the handling of the data of data subjects is considered high risk according to the General Data Protection Regulation

based on the above regulations. Individually, very easily, based on the range of data in the table

various tasks that sympathize with the party during its operation can become identifiable

the handling of the contact information of the parties involved together with the names and party affiliation

because of Violation of data confidentiality with high risks

involved parties

regarding his private sphere, since he belongs to a political organization - even if it may be from the past

- definitely reflects the political opinion of the given person.

Data relating to political opinion is Article 9 (1) of the General Data Protection Regulation

belong to a special category of personal data. The highlighting of these data is a

under the general concept of personal data, it is justified by the fact that such information is the data subject

they relate to more sensitive aspects of his life, therefore their disclosure is unauthorized

knowledge of it can be particularly harmful for the person concerned. This data is illegal

its treatment can negatively affect the individual's reputation, private and family life, it is disadvantageous

may be a cause or reason for discrimination against the person concerned.

Finally, the risks of data management are also increased by the fact that a large number of data subjects, more than 2,000, are

personal

data were processed together in the tables.

The responsibility of the data controller, i.e. in this case the Customer, is to comply with Article 32 (1)-(2) of the General Data

Protection Regulation

based on paragraphs that based on the nature, circumstances, purposes and risks of data processing, a

according to the state of science and technology, implement appropriate level of data security measures

finally. Among other things, these data security measures must guarantee that a

managed personal data should preferably not be made public without authorization, or should not be related to them

can be accessed without authorization.

Based on the judgment of the Authority, identification data and political opinion that can be linked to the data subjects

management of reflective data within the framework of Google Sheets, a free online service

in the form in which it was realized in the present case, it does not meet the high risk

the level of data security commensurate with the risks presented by data management.

Google Sheets is a free, web-based spreadsheet program offered by Google

It is part of the Google Docs Editors package. The application allows users to

create and edit files online while collaborating with others in real time

with users. Modifications can be tracked by the user using the modification display

with version history. The position of the editor has an editor-specific color and cursor

highlighted, and an authorization system controls what users can do. THE

documents can be shared, opened and edited by several users at the same time. THE

changes are automatically saved to Google's servers and a

system

automatically preserves version history so previous changes can be viewed and

they can be restored. THE

user local

to your computer, for example in PDF and Office Open XML formats.1

can be exported in formats a

files are different

1 See: - https://www.google.hu/intl/hu/sheets/about/;

- https://en.wikipedia.org/wiki/Google_Sheets

10

Handling the large amount of special personal data contained in the tables is very difficult in itself

it entails serious risks for the privacy of those concerned. The Customer is the high risk

in connection with data management, access to the tables was granted to the party's leading officials and

for its activists with the help of a link, since according to the party's internal principles, the activists can also directly

they can keep in touch with each other. In this way, even thousands of stakeholders could access the tables

online at once with a simple link, without any other restrictions. Because Google

Users can simply export and save files from the Sheets online service

to your local computer, therefore such a large number of access any other authorization control (e.g

password access to the table) in the case of provision without, it is very likely that

the occurrence that even unauthorized persons have access to the data, or that

a person entitled to it in advance sends it to others as well, or brings them himself

public. Nor to apply encryption to preserve the confidentiality of files

took place.

Without the application of additional appropriate control measures, it cannot be done by science and

from the point of view of the state of technology, it is sufficient to guarantee that it is very loose

access

personal data handled under measures should not be exposed sooner or later

public. The present is an example of the consequences of the lack of stronger security measures

also a data protection incident in the case.

Only in connection with the analysis of the file access log, the Customer could not establish that

whether they were accessed by an unauthorized external attacker, or if the files were made public

is it the result of an internal leak.

In the opinion of the Authority, if the Client stores the files in some internal, appropriate way

with encryption and

next to protection

authorization management and internal logging) would have been handled in a system (e.g. dedicated server), so

the data protection incident that is the subject of the report was also much less likely to follow

and the circumstances of its occurrence would have been easier to reconstruct.

Based on the above, the Authority determines that the Client is appropriate and proportionate to the risks

data security

by data processing in the absence of measures, violated the general

Article 32, paragraph (1) and points a)-b) of the data protection regulation, as well as (2) of this article

paragraph.

with traceable access control

with a password

(e.g.

2. Measures taken in connection with the handling of the data protection incident that occurred

Based on Article 4, point 12 of the General Data Protection Regulation, a data protection incident is considered a breach of security, which is the unauthorized disclosure of the processed personal data or related to them results in unauthorized access. From the point of view of the concept, it is the same as the security event relationship can be considered a key element. An event involving personal data is only that cases are considered data protection incidents if it can be caused by some kind of security breach connected, this is the root cause and there is a causal connection between the two. The safety damage may result from the security measures used to protect personal data incomplete, inadequate, possibly out of date, or due to their complete absence.

In the given case, the security breach was caused by the Customer not using the appropriate equipment technical and organizational measures regarding the data of party sympathizers

in order to preserve its confidentiality (see the provisions of point III/1 of the decision). Appropriate in the absence of security measures, therefore also the personal data of supporters and members containing tables, were removed from the from its management and made public by unknown persons on the Internet.

According to Article 33 (1) of the General Data Protection Regulation, a data protection incident is defined as controller without undue delay and, if possible, no later than 72 hours after it is becomes aware of a data protection incident, must report it to the supervisory authority. The incident reporting can only be omitted if the incident probably does not involve risk a regarding the rights and freedoms of natural persons. Assessing the risks associated with the incident it is the responsibility of the data controller.

Sensitive and accurate data that is classified as special personal data involved in the incident occurring during inclusive data management due to damage to security measures

a data protection incident is considered high risk. This is because of political activity

after the disclosure of the relevant data, the data controller's influence on their fate is complete

out of your control. Further confidentiality of the data management is not possible in full

guarantee in the future.

The client bears the risks related to their further fate due to the avoidance of data management

cannot take completely eliminating measures, the data – where appropriate illegal –

can no longer fully reduce the risks associated with its further treatment. The file sharing site

(in this case: https://ufile.io)'s subsequent request to delete the data reduces the

risks that the Customer took during incident management.

The Authority is also a factor that further increases the risks posed by the data protection incident

considers that access protection for the tables containing the special data of the data subjects (e.g.

could be accessed without a password), with just a link. Adequate data security

the application of measures would have reduced the risk of special data

third parties should not get to know me without authorization and they should not be made public.

The publication of the special data in comparison with the circumstances of the incident is the Authority

in his opinion, resulted in a high-risk data protection incident.

Based on the above, the Authority considers the data protection incident to be high risk

can be considered, therefore, if the data controller becomes aware of such a case, it must be reported

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

authority.

In view of the above, the Authority concludes that the data controller has complied with the general requirements

data protection

incident reporting

obligation, so no violation of law was established in this regard.

Based on paragraph (1).

Regulation 33.

existing

article

3. Findings related to the principle of accountability

Article 5 (2) of the General Data Protection Regulation defines "accountability

principle", according to which the data controller is responsible, contained in Article 5 (1) of the regulation

for compliance with its principles and must be able to demonstrate this compliance.

12

The Authority initiated an official inspection and then an official procedure in connection with the incident report

tried several times to inform the Customer about exactly what it was like

took measures to manage the incident and reduce the risks for those involved

however, despite the Customer's knowledge, he did not receive any answers regarding these.

Therefore, the customer did not prove to the Authority, despite repeated requests to provide data,

what exactly measures were taken in relation to the handling of the data protection incident

in order for the data management carried out by it to comply with the regulation from the point of view of the case

relevant regulations. Among other things, the Authority expected confirmation from the Client that it is

how did you transform the data management involved in the incident, so that in the future with the risks

apply proportionate data security measures to avoid a similar incident in the future

order (Article 32 of the General Data Protection Regulation), and that the persons concerned are subject to the high

in relation to a data protection incident with risk, how and with what content you were informed (general

Article 34 of the Data Protection Regulation).

Due to the lack of confirmation by the Client, the Authority cannot therefore establish that

Will the customer's data security measures in the future correspond to a level commensurate with the risks,

furthermore, what measures he took in connection with informing those concerned about the incident

Customer.

Due to the reluctance of the data controller, which can be blamed on him, the Authority also does not know the merits

to control the circumstances related to the handling of personal data, and this is also

leads to a serious reduction in the level of protection provided by the general data protection regulation, which ultimately, it puts those concerned in a vulnerable position.

Since the Client did not prove to the Authority that the regulation is relevant despite repeated requests measures taken to comply with its regulations, and therefore violated the general Article 5 (2) of the Data Protection Regulation.

4. The applied sanction and its justification

During the clarification of the facts, the Authority established that the Customer violated the general data protection regulation

- Article 32, paragraph (1) and its points a)-b) and paragraph (2),
- Paragraph 2 of Article 5.

The Authority examined whether the imposition of a data protection fine against the Customer is justified. E in the scope of the Authority, Article 83 (2) of the GDPR and Infotv. 75/A. it was considered based on § all the circumstances of the case.

In view of this, the Authority informs Infotv. Based on point a) of § 61, subsection (1), in the relevant part decided in accordance with the provisions, and in this decision, the Client to pay a data protection fine obliged.

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

In establishing the necessity of imposing a fine, the Authority considered the violations aggravating, mitigating and other circumstances as follows:

Aggravating circumstances:

- Data security deficiencies affected the personal data of a large number of stakeholders. [general Article 83 (2) point a) of the Data Protection Regulation]
- The data security gaps arose in connection with data management where special, political opinion data were handled together with contact data. On this illegal handling of data can negatively affect an individual's reputation, private and

family life, may be a cause or reason for discrimination against the person concerned,

moreover, it may also lead to misuse of personal identity. [general data protection

Regulation Article 83(2)(g)]

- The Authority regards the established data security deficiencies as a systemic problem

considers the incident to be not a one-time security deficiency or injury, but

can be traced back to the illegal handling of entire databases. [general data protection

Regulation Article 83(2)(a) and (d)]

- The Client did not cooperate with the Authority during the investigation of the case. THE

multiple requests for data provision verified by the Customer and procedural fines

despite this, he did not respond to the Authority's orders clarifying the facts. The Authority did not know that

to fully verify that those involved

reported risks accordingly

has it been reduced? [general data protection regulation Article 83 (2) point f)]

- When determining the amount of the fine, the Authority took into account that the Customer

violation committed by, thus Article 5 (2) of the General Data Protection Regulation

violation is the higher maximum amount according to Article 83 (5) of the regulation

is considered a violation of the fine category.

Extenuating circumstances:

- During the procedure, the Authority did not come to the attention of any information that would indicate

that the affected parties would have suffered any specific disadvantage or damage as a result of the infringement.

[General Data Protection Regulation Article 83 (2) point a)]

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

violation of the law related to the management of personal data. [83 of the General Data Protection Regulation.

Article (2) point (e)]

Other circumstances taken into account:

- The Authority on the violation of the Client according to Article 33 of the General Data Protection Regulation

found out based on his incident report. The Authority condemns this behavior - since a

did not go beyond complying with legal obligations - specifically as a mitigating circumstance

did not appreciate it. [general data protection regulation Article 83 (2) point h)].

14

- Based on the circumstances of the case and the Customer's statement, the Customer decided the risks

in terms of guaranteeing inadequate data security

technological solution

in addition to its application. However, the Authority could not verify it with the Client later

not because of its operation, but because of the reasons for choosing the technology

beer,

and whether the Customer has performed a preliminary risk analysis in this regard. The

the intentional or thoughtless nature of the data security breach is therefore expressed by the Authority

he could not evaluate it as an aggravating or mitigating circumstance. Not together with the Customer

on the other hand, he evaluated its operation under the aggravating circumstances. [general data protection

Regulation Article 83 (2) point b]

The Authority is responsible for general data protection when making a decision on the legal consequences

did not consider points c), i), j) and k) of Article 83 (2) of the Decree to be relevant.

The Authority is Infotv. Based on points a), b) and c) of Section 61 (2), the Customer is responsible for the decision

ordered the publication of his identification data, as it is

affects a wide range of persons, that is, through the activities of the Authority's public service organization

brought in connection, and also because of the involvement of special data, the public is the infringement

is also justified by its material weight.

ARC. Other questions

The competence of the Authority is set by Infotv. Paragraphs (2) and (2a) of § 38 define it, and its competence is

covers the entire territory of the country.

The Akr. § 112, and § 116, paragraph (1), and § 114, paragraph (1) with the decision

on the other hand, there is room for legal redress through a public administrative lawsuit.

The rules of the administrative trial are set out in Act I of 2017 on the Administrative Procedure

hereinafter: Kp.) is defined. The Kp. Based on § 12, paragraph (1), by decision of the Authority

the administrative lawsuit against falls within the jurisdiction of the court, the lawsuit is referred to in the Kp. § 13, subsection

(3) a)

Based on point aa), the Metropolitan Court is exclusively competent. The Kp. Section 27, paragraph (1).

Based on point b), legal representation is mandatory in a lawsuit within the jurisdiction of the court. The Kp. Section 39

(6) of the submission of the claim for the administrative act to take effect

does not have a deferral effect.

The Kp. Paragraph (1) of § 29 and, in view of this, Pp. According to § 604, the electronic one is applicable

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

hereinafter: E-administration act) according to § 9, paragraph (1), point b) of the customer's legal representative

obliged to maintain electronic contact.

The time and place of submitting the statement of claim is set by Kp. It is defined by § 39, paragraph (1). THE

information on the possibility of a request to hold a hearing in Kp. Paragraphs (1)-(2) of § 77

is based on.

The administrative lawsuit

law

(hereinafter: Itv.) 45/A. Section (1) defines. It is from the advance payment of the fee

Itv. Paragraph (1) of § 59 and point h) of § 62 (1) exempt the party initiating the procedure.

XCIII of 1990 on fees.

the amount of his fee is

15

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

fulfilled, it is enforceable. The Authority's decision in Art. according to § 82, paragraph (1) with the communication

becomes permanent. The Akr. Pursuant to § 133, enforcement - if it is a law or government decree

does not provide otherwise - it is ordered by the decision-making authority. The Akr. Pursuant to § 134 of

execution - if

law, government decree or local in the case of municipal authorities

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

Pursuant to § 60, paragraph (7), a specified action included in the Authority's decision

to carry out, for specific behavior,

obligation to

regarding the implementation of the decision, the Authority undertakes.

toleration or cessation

Budapest, April 22, 2022.

Dr. Attila Péterfalvi

president

c. professor