Case number:

Antecedent:

Object:

NAIH / 2020/1137

NAIH / 2019/4152

decision

ex officio

starting

privacy

official

procedure

DECISION

The National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority) shall

(Headquarters: […]) (the “Customer”)

on the protection of individuals with regard to the processing of personal data and on the

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

(EU) 2016/679 (hereinafter referred to as the General Data Protection Regulation) 32-34. contained in Article

ex officio data protection authority in the event of non-compliance with its obligations

procedure

1.

notes that

the. the Customer has violated Article 32 (1) of the General Data Protection Regulation,

thus, no appropriate technical and technical measures were taken in the field of data security

organizational arrangements by providing customer gateway access data

also stored the file containing it in printed form, which allowed it directly

the occurrence of the data protection incident.

b. Customer has violated Article 24 (1) - (2) of the General Data Protection Regulation

when dealing with internal data protection incident management

did not regulate notification to the supervisory authority

obligation.

2.

obliges the Customer to

the. a database containing customer gateway access data obtained from stakeholders

do not store on paper, only in electronic form, and the database is individual

back up your versions electronically.

b. Modify your internal privacy incident management policy to reflect this

the obligation to notify the supervisory authority.

3.

due to the above violation, the Customer shall be notified of the 30th day after the final adoption of this decision

within a day

HUF 500,000, ie five hundred thousand forints

order to pay a data protection fine;

4.

order the final decision without disclosing the identity of the controller

disclosure.

The fine is accounted for by the Authority's forint settlement account for the collection of centralized revenues

(10032000-01040425-00000000 Centralized direct debit account IBAN: HU83 1003 2000 0104

0425 0000 0000) must be paid by bank transfer. When transferring the amount, NAIH / 2019/4152

JUDGE. number should be referred to.

If the debtor fails to meet his obligation to pay the fine within the time limit,

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

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

the Authority's centralized revenue collection forint account

(10032000-01040425-00000000 Centralized direct debit).

Failure to comply with the notice under point 2 and fines and default interest under point 3

in the event of non-payment, the Authority shall order enforcement of the decision, the fine and the penalty payment.

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

Within 30 days, an action brought before the Metropolitan Court may be challenged in an administrative lawsuit. THE

the application must be submitted to the Authority, electronically, together with the case file

forward it to the court. The request for a hearing must be indicated in the application. The entire

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

HUF 30,000, the lawsuit is subject to the right to record material taxes. In the proceedings before the Metropolitan Court, the

legal

representation is mandatory.

EXPLANATORY STATEMENT

I.

Background, clarification of the facts

the. Public notice received by the Authority

The Authority received a public interest notification from an individual describing the

that he has been in possession of a list of natural persons and businesses (approximately 100)

contains various data. The list includes the full names, tax IDs, TAJ numbers,

birth information, their mother's name, and is available on the magyarorszag.hu website

client gateway contains their usernames and unencrypted passwords.

According to the petitioner, the list came into his possession in such a way that it was

in the garden of his estate, […] together with other rubbish that was blown up by the wind. THE

the list found was transmitted by the petitioner to the Authority in its original form.

The Authority initiated an official investigation into the notification under case number NAIH / 2019/1332

available data were not sufficient to judge that the customer gateway

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (hereinafter:

NISZ Zrt.) Whether the processing of personal data of natural persons was fully complied with

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

Regulation (EU) 2016/679 repealing Directive

Data Protection Regulation), in particular Articles 32 to 34. provided for in Article

During the official inspection, the Authority issued NAIH / 2019/1332/2. dated February 1, 2019

called on NISZ Zrt. to make a statement and provide documents. NISZ Zrt.

confirmed that the list does contain data relating to the Customer Portal, which are two

with the exception of a company and a sole proprietor are real and reflect the present state. To the Customer Portal

usernames and passwords belonging to the Central Customer Registration Register (a

hereinafter: KÜNY), in respect of which NISZ Zrt.

but the Ministry of the Interior (hereinafter: BM) is the data controller. Within the BM, the task is a

Deputy Secretary of State for Records Management of Personnel Records and Administration

It is provided by his department. In the case of the Customer Portal, KÜNY contains the following personal data:

natural identity data, citizenship, unique identification number of the applicant,

contact code, username, an unambiguous imprint of the login password and the person concerned

email address. According to NISZ Zrt., It is therefore included in the list found

passwords are not even handled by BM, only their irreconcilable imprint is included in the

in their records. The password can only be known by the person who completed the registration.

In the opinion of NISZ Zrt., The list is probably a customer database maintained by an accountant

may be because it even includes the tax ID, TAJ number, and ÜCC code, which is not

are related to KÜNY.

In view of the above, NISZ Zrt. Was not aware of the data protection incident and did not

In no way can the BM data management of him or her, who is entitled to manage KÜNY, be related

activities. The Authority therefore concluded that NAIH / 2019/1332/7. case number that a

based on the available information, there was no data protection incident at NISZ Zrt.

However, at the bottom of the published list, reference is made to an organization called […],

and that “companies / individuals registered under their name enter through their own gateways

everything."

[…] (Client) is engaged in accounting and has its registered office with the Authority

with the address of the forwarding complainant: […]. In view of this, the Authority, under a separate case number,

The initiation of a new official inspection on 16 May 2019 under case number NAIH / 2019/4152/2

decided regarding the data management of the Customer, as the available data were not available

are sufficient to assess whether the Client has fully complied with the general

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

b. For fact-finding orders sent by the Authority during official controls

given answers

1) The Authority NAIH / 2019/4152/2. by order no

to clarify the facts. The Client answered the questions asked in the order on time.

In its response, the Client acknowledged that it had been found by the public interest notifier and also to the Authority

the personal data belonging to its customers, which is actually managed by the Customer in the list sent

are located. The purpose of processing the data on this list has been established between the company and its customers

contracts for accounting, auditing and tax consultancy activities

fulfillment of obligations and contact with customers. These data are a

company’s customers voluntarily bring to light the signing of each assignment contract

their consent to the processing of the data for that purpose.

The personal data in the list is stored on the Client's own office server, for which it is exclusively

access to staff and the person in charge of IT tasks. Hosting with a password

protected. The list will be updated by the Customer in the event of a change in the data. During the upgrade, the list is one

shall be printed with the date of printing in handwriting and

along with the other lists, they are stored in a closed folder in chronological order. For this later possible

in view of the data checks required by the Customer. If you happen to be by accident

additional copies of the list are printed, it must be

"Grind".

He was not aware of the removal of the list from its management until the Authority's order was received

To a customer. In the Customer's judgment, the list is likely due to an internal act of bad faith

it could have escaped its treatment as both its electronic and paper-based storage is protected and sealed

takes place. Therefore, Customer has not previously identified a privacy incident

as he was unaware of it. In connection with the omission of the list, the Customer

plans to file a criminal complaint. In addition to the above, the exact circumstances under which the list was removed

the Customer is not aware.

2) The Authority sent another fact-finding order to the Client NAIH / 2019/4152/4.

number to which the Customer responded in due time. In it, he explained that in connection with the collection of data

has a separate privacy statement, by signing which they give their consent to the

to process customer data for the purposes set out above. A copy of this prospectus is provided by

Customer sent to Authority.

For the data in the list, there are 9 employees working in the office on the Client's server

he had access to it. They can access it for contract fulfillment and contact purposes

data. Access to the file is not logged. Access to the server

There are no special forced password policies for creating passwords

user can specify it individually.

The Client stated that after learning of the incident from the first order of the Authority, 12

all persons concerned were notified in person and by telephone within one hour.

At the Authority's request, the Client also stated that it had a data protection incident

with records. Incidents are reported in a text .doc also located on the central server

in an extended document. In the present case, he made an entry from the register

forwarded to the Authority by the Client.

c. Initiation of a data protection authority case and further clarification of the facts

In addition to the findings of the official inspection in the case, due to the alleged violation of the obligations set forth in Article 3234 of the General Data Protection Regulation by the Customer, Infotv. § 60

With regard to paragraph 1, the Authority decided to initiate an official data protection procedure in 2019.

July 16.

1) In addition to the findings of the official inspection in the case, further clarification of the facts has become possible therefore, the Authority will request a further inquiry, declaration and

NAIH / 2019/4152/7. number.

The Client responded to the above order on time. Required to access the office server in relation to the training of passwords, he replied only that they were in terms of their strength meet the "general requirements". Not yet on devices and system automatically checked and controlled password policy is established to process the incident however, it has been launched since then, but this requires a significant amount of financial and time.

In response to this question from the Authority, the Client stated that the server he was currently using acts as a file server. In order to create a new password policy, the so-called must be a domain controller promote the server and modify other components of the system accordingly. During this a security policy that provides enhanced security will be developed. In addition, individual users logging of access and access to data will also be established. In addition, the also user rights management and restriction of access to certain files can be configured in more detail in the system.

The Client has sent to the Authority its internal data protection policy, of which the provisions on the handling of data protection incidents. The rules cover incidents to register them or, in the case of high-risk

Article 33 (1) of the General Data Protection Regulation.

provisions relating to the obligation to notify under paragraph

In connection with requesting customer gateway data from data subjects, the Customer also provides this

stated that all day-to-day communication related to accounting (reporting,

declarations, queries) in the framework of centralized electronic administration, at the customer portal

through the current system. It arose during the transactions with the affected customers

The information used in connection with this is generated in the accounting office or is required here

for their use. In short, according to the Client, it is definitely up to the accounting firm to decide that

what action is required and is therefore required to enter the customer gateway and

for the administration of the data. The accounting firm therefore acts on behalf of the client through the client gateway

by managing their login details. According to the Client, this is how every accounting firm works. The future is

However, the customer will request the login details from the data subjects in a new, separate statement,

in which the conditions for the use of the data will be described in more detail.

2) After the above, the Authority will issue NAIH / 2019/4152/9. called for another statement

Customer to whom you responded on time.

To the Authority's question, the client gateway has .doc extension

file was provided with any access protection (e.g. password) the Customer did not respond on the merits.

Here he merely reiterated his earlier statement that the files, including the .doc file mentioned, were also included

stored on a file server. This server is used by each computer with its own password

they can achieve.

Customer has also stated that it does not currently have IT security

but is also being developed in view of the incident

van.

In the Customer's opinion, to periodically change the passwords of the affected customers' gatekeeper

is not their job, it is the privilege of that user. Regardless, it is the Customer

immediately informed the incident after becoming aware of the incident

stakeholders to change their gateway passwords. In addition, they were also informed about the

affected parties that if they were to suffer any damage as a result of the incident, the Customer would be complete

is aware of its responsibilities.

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

made the present decision in the case.

5

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.

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

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

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

take appropriate technical and organizational measures to ensure this

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

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

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

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

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

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

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

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

implement appropriate technical and organizational measures to address the risk

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

The risks arising from the processing

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

unlawful destruction, loss, alteration, unauthorized disclosure

or unauthorized access to them.

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

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

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

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

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

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

without undue delay after becoming aware of the data protection incident

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

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

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

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

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

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 the Act. It shall apply with the exceptions set out in Sections 103 and 104.
Act CXII of 2011 on the right to information self-determination and freedom of information. law
(hereinafter: the Information Act) pursuant to Section 61 (1) (a), the Authority shall
in the context of the data processing operations set out in
may apply the legal consequences set out in the Data Protection Regulation.
Pursuant to Article 58 (2) (b) and (i) of the General Data Protection Regulation, the supervisory
the data controller or processor acting under the corrective powers of the competent authority if
breached the provisions of the Regulation or Article 83
impose an administrative fine accordingly, depending on the circumstances of the case
in addition to or instead of the measures referred to in Paragraph 2 of the same Article
In accordance with point (d), the supervisory authority, acting in its corrective capacity, shall instruct the controller
or the processor to carry out its data processing operations, where appropriate in a specified manner and
bring it into line with the provisions of this Regulation.
The conditions for the imposition of an administrative fine are set out in Article 83 of the General Data Protection Regulation.
contained in Article. Infotv. 75 / A. § 83 of the General Data Protection Regulation.
taking into account the principle of proportionality
in particular in the legislation on the processing of personal data
or requirements laid down in a binding act of the European Union
Article 58 of the General Data Protection Regulation
in particular by alerting the controller or processor.
The Ákr. Pursuant to Section 104 (1) (a), the Authority shall ex officio in its area of competence
initiate proceedings if it becomes aware of a circumstance giving rise to such proceedings;
under paragraph 3 of the same paragraph, the ex officio procedure is the first procedural act
starts on the day of the execution of the contract, the notification of the initiation to the known customer may be omitted if the
the authority shall take a decision within eight days of the initiation of the procedure.

III.

Decision

the. The nature of the data protection incident and the action taken by the controller

1) On the basis of the facts revealed, the Authority has established that the data protection has taken place

According to the Client, the incident became known at the earliest when 2019.

On 20 May, the Authority was also informed of the details of the case in NAIH / 2019/4152/2. Facts

from the clarifying order. The case has not previously been classified by the Customer as a data protection incident,

since, he said, not bypassing a sheet of paper containing customer gateway data at all

he was aware. Upon contacting the Authority, the Client will file the case almost immediately for data protection

classified as an incident and attached to the general as part of the response to the request

from the incident register kept pursuant to Article 33 (5) of the Data Protection Regulation a

a copy of the entry and contacted him within 12 hours of becoming aware of it

all stakeholders and informed them of the incident.

7

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

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

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

in accordance with the principle of accountability1

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

freedoms. As the general rule is to report the incident to the authorities, this is not the case

an exception is also to be understood narrowly.

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

data processing, in this case the intended use of the devices.

identity theft or misuse of identity can result, so be it

considered risky. Data from the list leaked from the Client 's management (affected complete

name, tax ID, TAJ number, birth details, mother's name, magyarorszag.hu

customer gateway user names and unencrypted passwords available through the website)

and identity theft or misuse of identity may occur

use of customer gateway access without knowledge, other data stored there is unauthorized

getting to know.

Based on the above, the Authority considers that the data protection incident is fundamentally risky

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

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

authority.

The Client stated that in connection with the initiation of the official inspection only obtained

is aware of the occurrence of the incident and is therefore considered by the Authority to be official

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

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

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

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

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

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

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

as a result of which personal data have been compromised. ”2

The Authority will therefore refrain from requiring the Client to report the incident afterwards, as

an official inspection followed by a procedure clarified the circumstances of the incident and the action taken

measures. In the present case, the protection of the rights and freedoms of data subjects would not be enhanced

the subsequent request to report the incident has been closed

after.

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

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

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

privacy incident. According to recital 86 in the preamble to the Regulation, the main purpose of

so that the person concerned can also take the necessary precautions against the risks arising from the incident

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

[principles].

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

1

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

page 10.

2

in order to reduce The Authority in the present case classified the incident as a high-risk incident

which justifies informing 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 among the personally identifiable information

especially in the case of disclosure of username and unencrypted password pairs

nature (misuse of identity is very easy in the possession of this data),

whose risks can only be effectively mitigated if those concerned are aware of it

and may take any further action they deem necessary.

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

assessed in the opinion of the Authority if it is intended for entry into a system

username and password are unencrypted (or even inappropriate, outdated technical method)

encrypted). The main reason is that users have the same

data when using another service (mostly online or offline)

they can use. Users typically do not generate every single web

separate username and password for the service, but very often the same (or

certain versions) are used.

However, as the Client correctly assessed it already upon receipt of the Authority's first order, the
high risk of an incident and contacted him within 12 hours of becoming aware of it
therefore, the Authority considers that the general data protection rules have been complied with
obligations under Article 34 of this Regulation. In this regard, the Authority
makes no further request.

3) Finally, the Authority notes that Article 33 (5) of the General Data Protection Regulation
all data protection incidents, regardless of the risk classification, to data controllers
they must keep records. It shall set out the facts relating to the data protection incident,
its effects and the measures taken to remedy it. The Customer after learning
registered the privacy incident.

Prior to the Authority’s inspection, the Client was not aware that the list was leaked, so
personal data may fall into unauthorized hands. However, after the Customer becomes aware of it
contacted the parties concerned, informing them of the circumstances and liability
undertook after the possible consequences. In connection with the handling of the incident caused, the Customer a
In the opinion of the Authority, it took the necessary measures to issue a further request
therefore not justified.

b. Customer gateway is involved in data storage and incident management
data security measures

1) The Client is aware of the circumstances known in the clarification orders of the Authority
reviewed its internal processes and upgraded its data security measures (eg file storage,
use of passwords to access the server, etc.). The Authority will largely take these measures
accepts, but makes observations on some measures.

Data security measures taken before and as a result of the incident
the Authority makes the following findings.

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

unlawful acts involving personal data resulting from injuries. The concept

Thus, the relationship with the security incident can be considered as a key element.

With regard to the security of data processing, Article 32 (1) of the Regulation states that

taking into account, inter alia, the state of science and technology and the risks involved

data controller is responsible for ensuring that data security is properly technical and organizational

measures. Pursuant to paragraph 1 (b) of this Article, data security

measures are also designed to ensure that the systems used to process personal data and

ensuring the continued confidentiality, integrity, availability and availability of services

their resilience is guaranteed. Security is adequate under Article 32 (2)

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.

The Client stated during the procedure that the personal data listed in his office

stored exclusively on staff and IT tasks

person (9 people in total). The file itself is not just a client accessing the server

computers have been password protected. The purpose of data storage is a

performance of contracts with clients of an accounting firm. The list of Customer data is optional

updates when it changes. During the upgrade, the list will be printed in one copy with

the date of printing shall be recorded in handwriting and, together with the other lists, in chronological order

stored in a locked folder. You will need this in view of any subsequent data checks

according to the Customer.

In the Authority’s view, a measure to reduce the security of data processing is that

if the data controller on the server stored in the file of customer data using the above method all

for each data update, it is printed and stapled to a folder. Using this method in the file

stored customer data, including customer gateway resulting in sensitive and risky data management

the chances of unauthorized access to data increase. However, print the lists
no additional, evaluable in terms of the purpose and security of the data processing
does not add value, it is practically an unnecessary additional data management operation
results. The printing and listing of the list is therefore in accordance with Article 32 (1) of the General Data Protection Regulation.
and in particular point (b) thereof
measure.
The Authority considers that the storage of customer data is purely electronic and about it
making an electronic backup better guarantees the data security requirement and so on
compliance with Article 32 (1). With this measure, the subject of the case
the chances of incidents and the risk of data management can be reduced, so the Customer
it can also better comply with Article 32 (2).
An additional argument against printing the list is that of data protection arising from paper-based data management
the exact circumstances of the incident, so that exactly how the list could have come out of the Customer
has not been fully explored since then. This paper-based data management is thus
the detection and accuracy of any other similar privacy incidents that may occur to Customer
it may have hindered the exploration of their causes.
10
The Authority therefore concluded that the Customer had not complied with the General Data Protection Regulation
Article 32 (1) to (2) when dealing with the confidentiality of personal data processed
electronically available and up-to-date customer data as an unnecessary measure
also stored retrospectively on paper.
2) Finally, the Authority also finds in relation to the case that the Client is data protected
Incident Management Policy has been adopted with incomplete content. Incident management
The regulations do not contain any information on which data protection incidents are detected
cases must be notified to the supervisory authority.

Article 33 of the General Data Protection Regulation deals with the handling of data protection incidents

Paragraph 1 states that, as a general rule, they must be reported to the supervisory authority

unless the incident endangers the rights and freedoms of those concerned

viewed. Measures related to the reporting obligation from the incident management policy

they cannot be absent, as the regulation makes notification the main rule and only an exception

cases may differ. The rules accepted by the Customer shall nevertheless contain the

internal procedures for handling incidents, registration and informing those concerned

therefore only be considered incomplete in relation to the obligation to notify.

The Client can therefore be assessed by having developed its internal incident management policy

made efforts to comply with Article 24 (1) to (2) of the General Data Protection Regulation

for compliance. In this context, it shall be proportionate to its data management activities,

technical and organizational measures taken to ensure the security of data processing

applied an internal incident management policy as part of the measures. The Authority will assess this

However, as explained above, the Code needs to be supplemented by Article 33.

in order to comply with Article 1 (1).

The Authority therefore concluded that the Client had not fully complied with the general

Article 24 (1) to (2) of the Data Protection Regulation when the internal data protection

did not regulate reporting to the supervisory authority in its incident management regulations

obligation. In doing so, the Customer has violated these provisions of the Regulation.

c. Purpose, legal basis,

proportionality

The legal basis and purpose of the processing of access data by the customer gateway managed by the Customer is data

management

proportionality and the adequacy of the information provided to the data subject were not the subject of the present

proceedings.

The subject of this decision is solely the data security and incident management applied by the Customer

issues related to the specific incident that occurred. The Customer and

managing gateway access data for clients of other accounting firms in general

(as is customary market practice as claimed by the Customer) and any additional costs arising therefrom

data protection issues may later be the subject of a separate official investigation.

d. Findings concerning the sanction applied.

The Authority has examined the type of sanction it intends to impose on the Client

whether it is justified to impose a data protection fine on him. In this circle

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

subject to Infotv. § 61 (5), considered all the relevant circumstances of the case and

found that in the case of the infringement discovered in the present proceedings, the Customer 's warning and

is not in itself a disproportionate and dissuasive sanction, so a fine is justified

imposition. In determining the need to impose a fine, the Authority took this into account

above all, take into account that the data protection incident at the Customer is such

due to a data security vulnerability that has not only been specifically disclosed

personal data, but also all customer gateways handled by the customer on a paper basis

may compromise the security of contacts and other customer information. The Authority is therefore customers

access to another person's personal data is not secure, and the relevant data security

considers the inadequacy of the measures to be a systemic problem on the basis of which the infringement situation

existed at the data management Client even before the incident occurred.

The deficiency of the Privacy Incident Management Policy regarding reporting is also such

considered a systemic problem that may have been hampered by other regulatory controls and procedures

in accordance with the General Data Protection Regulation

treatment. In this context, in particular, the Authority shall take a risky view of the Client

incident pursuant to Article 33 (1) of the Regulation.

In determining the amount of the fine, the Authority took into account that by the Customer

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

constitute an infringement falling within the lower maximum amount of the fine. In addition, the

The following relevant factors were taken into account in setting the amount of the fine.

In setting the amount of the fine, the Authority took into account that the Client

Based on the financial statements for the year ended 31 January 2018 to 31 December 2018, this

had a total net sales of […] in. Based on the above, the amount of the fine imposed is an infringement

proportional to its weight.

The Authority has not previously established against the Client the processing of personal data

infringement.

As a mitigating circumstance, the Authority took into account the fact that the data protection incident

After being notified of the incident, the Customer shall be informed of almost all

33-34 of the General Data Protection Regulation. immediately took the measure provided for in Articles

investigated the incident and decided to take further data security measures

informed and registered the incident. By reporting privacy incidents

In addition to the deficiencies in the regulation relating to

did not reveal any further problems in its incident management practice. The incident management policy

however, its absence was assessed by the Authority as a systemic problem.

The Authority assessed the identified data security deficiencies as an aggravating circumstance

led to a high-risk data protection incident which

resulting in the personal data of about 100 natural persons (including

misuse of identity) have been disclosed. The shortcoming

thus high in terms of the risks to the rights and freedoms of data subjects

resulted in an incident of which the Client became aware only in connection with the proceedings of the Authority.

The Authority also took into account that the Client, however, after becoming aware of the incident

immediately proposed additional data security measures.

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

during the investigation of the case, although this conduct - as not in compliance with legal obligations

did not assess it as an express mitigating circumstance.

ARC.

Other issues

The powers of the Authority shall be exercised in accordance with Infotv. Section 38 (2) and (2a), its jurisdiction is

covers the whole country.

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

there is an administrative remedy against him.

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

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

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

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

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

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

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

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

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

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

hereinafter: E-Administration Act), the customer is legal in accordance with Section 9 (1) (b)

representative is required to communicate electronically.

The time and place of the submission of the application is Section 39 (1). THE

Information on the possibility of requesting a hearing is provided in the CM. Section 77 (1) - (2)

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

Fees. law

(hereinafter: Itv.) 44 / A. § (1). From the advance payment of the fee is

Itv. Section 59 (1) and Section 62 (1) (h) shall release the party instituting the proceedings.

The Ákr. According to § 132, if the debtor does not comply with the obligation contained in the final decision of the authority fulfilled, it is enforceable. The decision of the Authority With the communication pursuant to Section 82 (1) it becomes final. The Ákr. The Ákr. Section 133 enforcement - if you are a law Government decree does not provide otherwise - it is ordered by the decision-making authority. The Ákr. § 134 enforcement - if by law, government decree or municipal authority matter local government decree does not provide otherwise - it is carried out by the state tax authority. The Infotv. Pursuant to Section 60 (7), a specific act included in the decision of the Authority obligation to perform, to behave, to tolerate or to stop implementation of the decision shall be carried out by the Authority.

Budapest, January 24, 2020

Dr. Attila Péterfalvi

President

c. professor