Case number: NAIH / 2020/1160/10

History: NAIH / 2019/7105

Clerk:

Object:

decision

ex officio

starting

privacy

official

procedure

DECISION

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

Electronically by Távközlési és Szolgáltató Kft. (Registered office: 1134 Budapest, Váci út 35., company registration number:

01-09667975).

in connection with the data protection incident reported on 25 September […] a

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

Articles 5 and 32 to 34 of Regulation (EU) 2016/679 (hereinafter referred to as the General Data Protection Regulation). in its

articles

ex officio breach of data protection obligations

in official proceedings

1.

notes that

the. the Customer has violated Article 5 (1) (b) of the General Data Protection Regulation

('Purpose limitation') and (e) ('limited storage capacity') when the data protection

an incident-related test database originally set up for troubleshooting purposes is required

after running the tests and correcting the error, it was not deleted, so it stored a large number

customer data was obtained in the following […] period without purpose and in a manner suitable for identification

for storage in used systems. The absence of such a measure directly allowed the

the occurrence of a data protection incident and the availability of personal data.

b. Customer has violated Article 32 (1) - (2) of the General Data Protection Regulation, thus

not proportionate to the risks to the security of data management

technical and organizational measures, by:

-

the content manager it uses ([…]) has been known for more than 9 years, adequate

could otherwise be detected and repaired

access to the incident through the publicly available digi.hu website

databases;

-

with regard to personal data involved in a data protection incident ([…]) no

applied encryption, which greatly exposes the risks of the incident

increased it.

The lack of these measures directly allowed it to be stored in databases

customer data has also been made available by an ethical hacker who has carried out the attack

through vulnerabilities.

2.

obliges the Customer to review all personal data processed by him

whether encryption is justified and

inform the Authority of the results!

3.

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

within a day

100,000,000 HUF, ie one hundred million HUF

order to pay a data protection fine;

4.

order the final decision by publishing the identity of the controller, but the

disclosure of business secrets.

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

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

0425 0000 0000) must be paid by bank transfer. When transferring the amount, NAIH / 2020/1160

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 of the application addressed to the Metropolitan Court in an administrative lawsuit

can be challenged. The emergency does not affect the time limit for bringing an action. The application to the Authority

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

The application for maintenance must be indicated in the application. During the emergency, the court is hearing

acting outside. For non-personal tax exemptions, judicial review

the fee for the proceedings is HUF 30,000, the lawsuit is subject to the right to record fees. Before the Metropolitan Court

legal representation is mandatory in these proceedings.

EXPLANATORY STATEMENT

I.

Background, clarification of the facts

the. During the incident report and official control received by the Authority

established

1) The Data Protection Report notified electronically by the Client on 25 September 2019

initiated an official investigation into the incident on October 8, 2019, as reported

the information provided was not sufficient to judge that the Customer fully complied

whether it has complied with its obligations under the General Data Protection Regulation, in particular Articles 32 to 34.

provided for in Article

According to the announcement, the Customer became aware on September 23, 2019 at the latest that

an attacker had access to the vulnerability through the www.digi.hu website

about […] the personal data of the data subject, who are the majority (approx. […] persons) of the Customer's customers

and subscribers, and a smaller number (approximately […] people) were subscribers to its newsletter. Customers, subscribers

personal data included the names of the data subjects, the name of their mother, their place and date of birth,

address, ID number (if applicable), e-mail address, landline and

mobile phone number.

During the official inspection, the Authority issued NAIH / 2019/7105/2. and NAIH / 2019/7105/4. case number

by its orders, the Client was requested to make a statement and provide documents. Customer Statements

the Authority has established the following during the official control.

2) Customer became aware of the attack as indicated by the attacker (ethical hacker)

to him […]. In his signal, the attacker indicated that, he said, only the affected database was one

requested as evidence and his intentions were of an assistive nature, so the technical nature of the error

explained to Customer. The Customer has subsequently corrected the error, […].

Most of the data involved in the incident (approximately […] people) was generated for testing purposes on […].

They were part of a database called […]. The reason and purpose of creating the test database is

Attempted by scanning client log files, system alerts, and mail

to reconstruct. Because the log files and alerts for the assumed upload time are no longer

were available so it was not possible to reconstruct the events clearly

To a customer. An email from a test colleague […] revealed that […] had an error that

during which the web servers did not reach the database servers. As a result, the

subscriber data is no longer available. Customer assumes this error is temporary

The data, the subscriber data, have been uploaded to the test database in order to eliminate them

to ensure its availability.

The source of the data loaded into the above test database created to resolve the error is

It consisted of personal data previously provided by the data controller's customers. Customers are different

they provided their personal information online or through other sales channels during their claims

across […]. It had the latest […] date resulting in data loaded into the test database

equipped with. In this database, approx. […] Was data provided by a natural person

can be found.

After the above error is resolved, access is restored to the test database

data should have been deleted, but this was not done due to omission. These data a

was unaware of its availability through the above vulnerability until the attacker announced it

To a customer. Access to the data by the attacker could not be detected by the Client

(e.g., based on a network security device signal) before being called by the attacker himself

attention.

In addition to the test database, the attacker had the opportunity to discover the vulnerability

to access another database […] behind the digi.hu website maintained by the Customer, which is

contained the personal data of those who subscribed to the newsletter. Here approx. […] Natural

data provided by the person (name, email address) was found. Based on the tests in this

However, specific personal data stored in a database may not be detected as unauthorized

access according to the Customer. However, due to the vulnerability, the risk of access to this data

also existed.

3) The specific vulnerability was listed on page […]. It was here through the “sort field”

exploit the vulnerability of the website. The reason for the unauthorized access error is that

3

a vulnerability exists in the […] 1 content management system used by Customer that

exploited by the attacker. The vulnerability has been known and available for more than 9 years

there was also a patch that was not previously installed by Customer. This is because of the repair

was not part of the officially released fix packs for the software. After the incident

fix pack 2 is installed.

Customer will not gain additional unauthorized access to the affected data through this vulnerability

showed up. No other circumstance suggested that the data might have been accessed by anyone else

outside the ethical hacker.

4) Customer has also informed the Authority to prevent similar data protection incidents

it regularly checks the databases it manages in order to avoid any specific purpose

personal data is processed / stored. Databases are also provided from time to time

cleans, checks their security, identifies related applications, and

data controllers. In addition, as a result of further external investigation, it will be considered higher

obtain and operate a level firewall.

Customer has internal policies based on the applications it uses

they must be kept up to date and checked regularly for this purpose. The incident

the latest version of the […] system (with which the affected database was managed)

applied an unofficial patch to fix the vulnerability, but it did not. Maga a

vulnerability was in it by the way […]. In this regard, the Client submitted that since the

there are a lot of unofficial fixes for the official version that you can't check.

Regarding the use of open source content management, Customer […] said that

chose this system because it is free, widely used around the world as well

a software that is constantly tested and supported.

Customer […] shall regularly perform vulnerability testing of the systems it uses

using […]. However, this investigation is the occurrence of a privacy incident

did not cover the digi.hu website until the date of Following the incident, the investigation was extended by

Customer to this website as well.

[…]

The attacker who reported the vulnerability […]. The test database named [érintett] involved in the incident

Customer also deleted in the meantime.

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

1) In addition to further clarifying the facts, Articles 5 and 32-34 of the General Data Protection Regulation in this case apply.

any further breach of the obligations by the Customer under Articles

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

CXII. With regard to Section 60 (1) of the Information Act (hereinafter: the Information Act), the

decided to initiate official proceedings on 16 December 2019.

1

[…]

2

[…]

4

In addition to the findings of the official inspection in the case, further clarification of the facts has become available

necessary, the Authority should therefore amend NAIH / 2020/1160. and NAIH / 2020/1160/3. with his orders no

called on the Client to make statements and provide documents, for which the deadline was reached

answered. Based on the Client's statements, the Authority clarified the official inspection

In addition to the circumstances, it found the following during the official procedure.

2) The Customer is presented in detail with the help of a diagram and description involved in the incident

the structure of servers and other network elements and the location of databases. Based on these, the

data files affected by the incident […] 3 […] were available on the affected network […]

(see figure below).

[…]

Used by Customer to create and further manage the database.

The personal data stored in the incident […] has not been encrypted Customer Statement

Based on. This is because the […] requirement for encryption does not appear internally

regulations.

According to the Client, the database […] did not consider it justified either because it was personal

data protection by restricting access and allocating rights in principle

the use of such encryption in the usability of the databases and

may cause a problem with its operation. The cause of the specific problem was not explained in detail by the Customer.

Otherwise, the use of encryption in the IT systems of the Customer

appears in general in its regulations called […]. Relevant points of the regulations

sent by the Client at the request of the Authority.

3) At the request of the Authority, the Client described in detail how the attacker managed to implement it

attack and access personal data stored in the database […]. The method itself is a

attacker introduced to the Customer. Based on these, the attacker ran a so-called […] attack on

on the affected digi.hu website. Executing this attack is, in the opinion of the Customer, time consuming

task and may only be performed intentionally with the intention of unauthorized access

implementation requires a high level of technical knowledge. The attack is carried out by the attacker

A vulnerability has been reported on […], through which […] has become available and can be listed.

a total of […] rows of […] in the test database.

At the request of the Authority, the Client explained in detail that the incident involved two separate

for a database, exactly what categories of data were handled, what that data was

the purpose and legal basis for the processing of the data and the exact number of personal data of the data subject

treatment.

- Test database named […] containing subscriber data: name of the data subject, date of birth

name, mother's name, place and date of birth, address, identity card number, if applicable

personal number, e-mail address, landline and mobile phone number, bank account number,

data related to the contract, data related to the service used. The

the purpose of data management in this case is to conclude a subscription contract. Data management

Legal basis: Article 6 (1) (b) of the General Data Protection Regulation (data processing

necessary for the performance of a contract to which one of the parties is a party). The

3

[…]

5

-

a total of […] personal data of the data subject were processed in the database. This number is the Data Controller

[…]% of its retail customers.

Live […] containing the data of the newsletter subscribers, can be linked to the digi.hu website

database: name and email address. The purpose of data management in this case is the data subjects

with the offers offered by the Client for the purpose of acquisition (dir

marketing). Legal basis for data processing: Article 6 (1) of the General Data Protection Regulation

(a) (the data subject has given his or her consent to one or more of his or her personal data)

for a specific purpose). A total of […] people are affected in the database

data were processed. This figure represents a total of […]% of the Data Controller's retail customers.

The Client forwarded it to the Authority by handling the data files affected by the incident

internal data protection incident management procedures.

4) The Client has explained to the Authority the technical vulnerabilities on the digi.hu website

description that the attacker also provided in his message.

An e-mail message from an ethical hacker describing the vulnerability reveals that […]

in addition to the database ([…])

The personal data of the data subjects subscribing to the newsletter on the digi.hu website

In addition, it contains access data to the interface of the digi.hu website. In this, it is called […]

the database also contains the data of the […] partial / full administrator user named […]

can be read according to the letter from the ethical hacker. This data includes […]. These data are

According to the message, they can allow access to the administration interface of the digi.hu website.

Based on the above, the ethical hacker e-mail message that the databases involved in the incident and

personal data is illustrated in the table below:

Database name

[…]

Number of stakeholders

[…] Subscriber

[…] Subscribing to the newsletter

Data type

Name, birth name, place of birth and

time, mother's name, email address, password,

mobile phone number, bank account number,

ID number, ownership

(owner or tenant), method of payment,

willingness to pay

data (eg debt collection), by contract

related

data,

used

service

type,

service

start / end date.

Newsletter subscribers: name, e-mail address

[…]

[…] Partial / full

system administrator

Administrators: […]

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

made the present decision in the case.

6

II.

Applicable legal provisions

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

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

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

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

the general data protection regulation applies to data processing.

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

"security incident" means a breach of security which

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

loss, alteration, unauthorized disclosure or unauthorized disclosure

results in access.

According to Article 5 (1) (b) of the General Data Protection Regulation, personal data

collected for specified, explicit and legitimate purposes and not processed

in a way incompatible with those objectives; […] ("Purpose limitation").

According to Article 5 (1) (e) of the General Data Protection Regulation, personal data

should be stored in a form that identifies the data subjects only for personal use

allows the time necessary to achieve the purposes of data processing; […] (“Limited

storability ”).

Pursuant to Article 5 (2) of the General Data Protection Regulation, the controller is responsible for

must be able to comply with the principles set out in

(‘accountability’).

Pursuant to Article 17 (1) (a) of the General Data Protection Regulation, the data subject is entitled to

that, at his request, the controller deletes his personal data without undue delay

data, and the controller is obliged to provide personal data concerning the data subject

delete without undue delay if […] personal data are no longer required from

for the purpose for which they were collected or otherwise treated.

According to Article 32 (1) (a) 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 an adequate level of data security, including, where appropriate, the

pseudonymisation and encryption of personal data.

In accordance with Article 32 (2) of the General Data Protection Regulation

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 Art. 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.

8

III. Decision

the. Applicability of the General Data Protection Regulation

Pursuant to Article 99 (2) of the General Data Protection Regulation, the Regulation will apply from 25 May 2018

should be used. The test database named [érintett] affected by the Privacy Incident is Customer

was created on the basis of its statement […] for testing and troubleshooting purposes.

The database called […], which contains data that can be linked to the digi.hu website, is direct marketing

providing information on newsletter subscribers and access to the website interface

contained administrator data that was not test but live, up-to-date data.

The Customer acknowledges that one of the vulnerabilities on the digi.hu website has been exploited for the above two

databases

can be accessed from the outside by unauthorized access at the earliest on September 23, 2019 notified of security

from an ethical hacker who uncovers an error. Data management affected by the incident, namely customer data

storage in the databases affected by the incident, the general data protection regulation applies

continued after his divorce. Therefore, both Article 99 (2) and

shall apply in accordance with the substantive requirements set out in Article 2 (1)

requirements of this Regulation.

In addition to the above, it should be noted that the General Data Protection Regulation is a data protection incident

the incident

Acquisition is the relevant date, as the legal consequences required by this Regulation are

binds to a date. In this respect, the fact that it is involved in the incident and is insufficient

when a test database managed using data security measures was created

and when data collected from data subjects is included is not a relevant factor. That's it

incident and an inadequate level of data security

risks to the rights and freedoms of data subjects even after the Regulation becomes applicable

they existed.

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

Based on the facts revealed, the Authority concluded that the data protection incident had taken place

the Client, in his own words, became aware of it at the earliest when it was disclosed to the person concerned

An ethical hacker conducting a vulnerability investigation on the digi.hu website informed him by e-mail

[…]. Previously, Customer was unaware of the vulnerability. By the attacker

the vulnerability analysis performed, the listing of the categories of data in the relevant databases, and

the Customer was unable to access the data stored in the test database automatically

detect the incident and the vulnerabilities that lead to it, only the ethical

was informed by a hacker.

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

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

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

considered. In connection with the Client's incident reporting and clarification of the facts, it can be stated that a

for a test database created for testing and troubleshooting purposes containing personal information a

Vulnerability available to the attacker through the digi.hu website maintained by the Customer

managed to access it. Unauthorized access to personal data is therefore one

IT security vulnerability, which is thus data protection

resulted in an incident.

9

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

the incident 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 accountability4

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 storage of data of retail customers and system administrators,

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

considered risky.

Data stored in the database created by the Customer for testing and debugging purposes (name of the data subject,

birth name, mother's name, place and date of birth, address, identity card number,

occasionally personal number, email address, landline and mobile phone numbers, payment and banking

data related to the requested service)

identity theft or identity theft.

Another one available through the security breach, which can be linked to the digi.hu website, is named […]

for data stored in the database (newsletter and administrator data)

an ethical hacker also indicated the vulnerability of this data, although he did not request specific data,

listed only the types of data available for administrators ([…]). Regardless, a

shortcomings in security measures, such as protection against unauthorized access

an adequate level was also maintained for these data.

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

therefore, if the controller becomes aware of such a case, it must notify it

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

notification was made by the Data Controller to the Authority on 25 September 2019, so this is the direction

within 72 hours of becoming aware of the incident. The Authority shall:

has therefore not found an infringement of the obligation to notify.

In connection with the incident, the Data Controller described the possible adverse consequences

mitigation measures. Based on these purposelessly managed test database

deleted and installed the patch that is present on the […] system that you are using

eliminated the vulnerability. The Customer has already applied such prior to the occurrence of the incident

organizational measures that sought to filter out unnecessary, untargeted treatment

data, databases, however, the relevant test database has not been included in this connection before

for detection. Customer has also stated that it will consider higher level firewalls

to increase the level of protection and anyway

regular vulnerability scans and […] will be extended to the digi.hu website in the future.

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’).

4

10

c. Data security measures related to the storage of data affected by the incident

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. Paragraph 1 (a) of this Article shall mean, where appropriate, personal

aliasing and encrypting data.

When determining the appropriate level of security pursuant to Article 32 (2)

account shall be taken of the risks arising from the processing, in particular:

personal data transmitted, stored or otherwise handled is accidental or unlawful

destruction, loss, alteration, unauthorized disclosure

or from unauthorized access to them.

1) Information provided in the incident report and official control during the procedure

Based on the facts established in., the occurrence of the data protection incident can be traced back to:

in the […] system used by the Customer for content management, with which the incident is involved

databases were also managed - there was a long - known and

repairable vulnerability. Customer says this vulnerability has not been corrected by

until an incident occurs because the service pack is not part of the software

officially issued version. Customer will not follow […] available unofficial fixes,

does not monitor it due to the number of unofficial patches for the software

because of what he says he has no opportunity, no capacity. Customer will conduct regular vulnerability testing

in the systems managed by it, however, until the occurrence of the incident, digi.hu

did not cover the website.

In accordance with Customer's IT Security Policy […].

Management of customer data affected by the incident - Annex III./b. also in accordance with the provisions of

considered risky based on the content of the data categories. Significantly increasing the risks

factor is that the database managed by the Customer contained a large number of personal data of the data subject

can be found:

- […] test database: […] affected subscriber, the data controller's retail customers

[…]% of total,

- Database named […]: […] affected subscribers, for the total number of retail customers of the Data Controller

[…]%, In addition […] partial / full system administrator can be linked to the digi.hu website

access details.

These are, therefore, a total of […], more than […] of the Data Controller's retail customers,

sensitive data processing affecting a significant number of stakeholders in proportion to the Hungarian population,

which, pursuant to recital (75) of the General Data Protection Regulation, are concerned

significant risks to their rights and freedoms. Pursuant to Article 32 of the Regulation

the obligation of the data controller to take data security measures proportionate to the risks

apply.

The testing and debugging activity performed by the Customer is the customer database named […]

otherwise it would not be a problem to report at the same time as such data processing

security measures proportionate to the risks are also applied. Customer internal

its information security regulations also contain requirements regarding the use of

systems, the risks need to be assessed in advance and mapped out

vulnerabilities and available fixes, as well as appropriate encryption

apply. In addition, systems should be regularly inspected for potential vulnerabilities

to explore.

2) The Client has sent to the Authority the technical vulnerabilities on the digi.hu website

description that the attacker provided to him in his message. IT security expert of the Authority

examined the vulnerability's description of the vulnerability and reported it by Customer

information. This is described in NAIH / 2020/1160/5. case information security experts

opinion, which with the Client in accordance with Ákr. Pursuant to Section 76 of the NAIH / 2020/1160/7. number

described by order.

According to the expert opinion, it can be concluded that it was done by the attacker

based on a vulnerability assessment, this is a […] vulnerability. This type of error is characterized by

that […]. However, there are web vulnerability applications that are out

they can also filter […] vulnerabilities automatically. Such e.g. also referred to by the Customer

and used […] are also widely used for this purpose. Use of this […] software

otherwise does not require a particularly "high level of IT knowledge" or code-decomposition ability,

they are moderately proficient in IT security issues of interest to the subject

a person can also master it after some practice and time.

The parameters of the vulnerability test described by the attacker show that the vulnerability is […]

was found through. On this link, […] was vulnerable, meaning […] could be exploited

[…] Vulnerability. According to the expert study, it can be successfully extracted from the relevant databases

(Databases named […]). Additional data may be included within these

get to know if […] so they can get to know […] (specific personal data).

Storing sensitive data in plain text in the database

high level of security problem according to expert opinion, which is appropriate encryption

can be eliminated by using. It can be prevented by using the […] mentioned by the Customer

would have been to know the specific contents of the database concerned.

An email from the ethical hacker describing the vulnerability also revealed that […]

also the data of a partial / full administrator user from the database named […]

can be read. This data includes […]. Such a sensitive, administrator level

access to data also greatly increases the risk of an incident,

since possession of this data is easy to commit identity theft or even more

unauthorized access to data.

3) Customer has submitted comments on the above IT security opinion and

comments to the Authority after it has been approved by the Authority in accordance with Art. Pursuant to Section 76 a

NAIH / 2020/1160/7. by order no.

Based on these, the Customer again stressed that the ethical hacker is only one of the […] database

requested as evidence and described it in a letter and no further unauthorized access

evidence. The Authority does not dispute this fact in the present decision. At this point in the decision (Annex III),

Chapter / c. Irrespective of this circumstance, the data security vulnerabilities assessed in

in relation to the personal data processed in the databases concerned and therefore

the risks posed to the data subjects can be linked to all the personal data processed.

12

Customer also highlighted the high level required to detect the vulnerability

IT knowledge is supported by its time-consuming and complexity. The Authority shall

notes that the mentioned software for detecting vulnerabilities is automatic

are able to detect vulnerabilities easily (for free if necessary) for anyone

are therefore not specific to the user

their use.

The client's statement reiterated that due to access control to the database

theoretically secured by authorization, so encryption was not considered justified

application. Furthermore, the encryption of the database table […] […] is incomprehensible according to the Customer

as there were some of the personal data concerned (eg names, addresses, telephone numbers),

whose encryption would have caused a problem in the usability of the database in the present case, and

operation. The reasons for this were not further specified by the Customer. The Authority hereby

See Annex III to this Decision. Chapter c. in point 5).

Finally, the Client drew the Authority’s attention to the fact that the […] employee (administrators,

administrators, users) […]. The Authority does not dispute the above, but notes that

nevertheless, the possibility of accessing […] data is in itself a serious security breach

considered as a risk factor.

4) The failure of the vulnerable content management system ([…]) used by the Customer is 9 years

it was well known along with the method of correcting it. Related entries a

have been publicly announced on the official website of the software.5 There is an error

The fix pack was not officially made, but an unofficial fix was available

it was publicly and free to anyone.

The vulnerability is related to the vulnerability investigation of the digi.hu website by an ethical hacker

for detection. To test this, the Customer also used to check other systems […]

software is also suitable. However, these inquiries were previously made in connection with the Website by the Customer

he could not detect the vulnerability either. Publicly available, visited by customers

website in connection with the omission of security investigations thus allowed for the vulnerability

do not shed light until the specific incident occurs. The regular

a vulnerability scan could have detected the error, as evidenced by an ethical hacker scan.

In this regard, a software component to repair an existing vulnerability is “no

is an irrelevant factor as to the existence and detectability of the error

it doesn't matter. Increased attention and action will be taken on the vulnerabilities in the systems used

required by the Client's internal regulations.

It is publicly available on the Internet and can be visited by (possibly a large number of) customers

Preparedness for potential vulnerabilities in relation to websites is expected to increase

maintainers. This is the state of science and technology and the cost of implementation

would not be of particular concern to the Customer in the present case, subject to

position in the market. The website and all other systems available on the Internet are regular

the Client also took action to require a vulnerability assessment after the incident, acknowledging this

the need for.

The level of security of the management of the databases involved in the incident was therefore not adequate

the requirements of Article 32 (1) to (2) of the General Data Protection Regulation

5

[…]

13

known security error that can be filtered out and repaired, as well as the vulnerability of the digi.hu site

failure to investigate allowed unauthorized access to personal data.

5) The Client also informed the Authority that it did not take place in the relevant databases

to apply encryption to personal data ([…]). This is also the message sent by the ethical hacker

confirms that the specific data have been retrieved from the database

personal data in readable form. To prove this, the ethical hacker asked the person concerned

[…] A row of a database that you also provided to the Customer.

Customer's IT Security Policy […].

The databases were created by Customer using the […] software, which allows

to encrypt data […]. In relation to the technology used, the personal data processed a

therefore, it was possible to use encryption, and its use should not mean any additional costs. The

However, according to the customer's statement, the […] databases it manages will be decrypted

did not use this option for the databases involved in the incident.

The reason given by the Customer is that the protection of personal data is accessed

such encryption is in principle ensured by restrictions and appropriate allocation of rights

may cause problems with the applicability and operation of the databases. THE

possible problems were not specified by the Customer.

However, in the absence of the use of encryption, the incident is involved in the present case

the vast majority of personal data stored in databases is unreadable, unauthorized

became known. That fact is the case with regard to the data protection incident that has taken place

significantly increased the risks to those affected.

The encryption of personal data is generally governed by Article 32 (1) of the General Data Protection Regulation.

It is also mentioned in paragraph 1 (a) as an appropriate security measure.

However, the Customer did not specify why the encryption of the database […] is considered specific

problematic in relation to data management, but in the absence of this it should

to protect against the leakage of sensitive and large amounts of personal data. Encryption

the exact reasons for its non-compliance under Article 5 (2) of the General Data Protection Regulation

you need to know.

Due to non-encryption of the incident occurred, in addition to the security applied

significantly increased the risks of the measures to those concerned, and therefore the general

Article 32 (1) (a) of the Data Protection Regulation and its own internal

In order to comply with its rules, the Authority has requested the Client to

to review all persons it handles in order to reduce the risks

a database containing data on whether encryption is justified in them

and the results thereof, in accordance with the principle of accountability.

inform the Authority.

6) In view of the above, the Authority therefore concluded that the Client had not complied with the

Article 32 (1) to (2) of the General Data Protection Regulation, with regard to data security

related legal requirements.

14

d. Compliance with certain principles for the management of the test database affected by the incident

1) For the purpose referred to in Article 5 (1) (b) of the General Data Protection Regulation

The principle of "confidentiality" requires that the collection of personal data be limited, clear and

for legitimate purposes and should not be treated as incompatible with those purposes

way.

According to the related opinion of Working Party 29 on Data Protection (WP203)

the essence is to prevent the data from being used for purposes for which the data subjects do not

may anticipate, protest, or otherwise be unsuitable for such purposes

to achieve. The principle is made up of two further parts, namely the goal first

and, secondly, the associated use

obligation.

The Customer indicated the purpose of creating the test database affected by the incident in that […] an error occurred that

caused the subscriber data to become unavailable. This is a mistake

was created for the purpose of repairing the [[]] data subject's retail customers

[…]% of the total data provided during the conclusion of the subscription contracts

test database containing. The purpose of creating this database (bug fix) is therefore separate from the

from the purpose of the original processing of personal data (performance of the contract). Bug fixes as standalone
the purpose of the data management may be legitimate, but this separate data management must also comply with the
requirements of the General Data Protection Regulation, including, inter alia, purposeful data processing
principle.
The goal of error correction in creating a test database lasts as long as the error itself
has not been remedied by the Data Controller. Once the error has been corrected, it is isolated
the purpose of the processing also ceases, so that Article 17 (1) (a) of the General Data Protection Regulation
The test database containing personal data had to be deleted, subject to the provisions of point
would be. Storing the database after the error has been completed has no data management purpose,
to which the Client himself referred in his replies to the Authority (see:
NAIH / 2019/7105/4. dated 28 November 2019
paragraph 4 of its declaration).
Therefore, the purposeless storage of a database containing a large number of sensitive customer data will be […], a
from the time the fault was rectified until the time the incident occurred. The Customer is responsible for this data management
therefore infringed Article 5 (1) (b) of the General Data Protection Regulation.
the principle of ‘purpose limitation’ mentioned in
2) The “limited
The principle of "storage of personal data" requires that personal data be stored in such a form
identification of data subjects for the sole purpose of processing personal data
allow the necessary time.
Closely related to the principle of purpose limitation, this principle is obsolete, no longer for any purpose
prohibits the storage of personal data that cannot be used. However, the principle is
retention of data in a way that identifies the data subjects
limits. You still have the option of storing anonymized data
data controller, but in such a way that it cannot be
draw conclusions for the data subject and identify them further.

The purpose is personal data processed in a database created by the Customer for troubleshooting purposes
unchanged after its realization, so that the data subjects were stored in a way that could be identified.
The identity of the data sent to the Customer by the ethical hacker
also confirmed a vulnerability message. The readability of the data, so the stakeholders
access to and identification of your data is otherwise encrypted
as in the previous paragraphs of the decision
it has been established.
Thus, the Customer has created for the purpose of troubleshooting, containing the data of the data subjects
test database for the identification of those involved in the period after the troubleshooting and then […]
infringed Article 5 (1) (e) of the General Data Protection Regulation.
the principle of 'limited storage capacity' referred to in
e. 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 considered the infringements
aggravating and mitigating circumstances as follows:
Aggravating circumstances:

-

A Customer Privacy Incident for a Data Security Vulnerability
tracing back to which free repair has long been available on the market,

and the vulnerability could be easily detected even by a third party, so that

to prevent exposure to unauthorized access to data to the Customer a

would have been an option for a very long time if the risks were properly assessed.

-

The large amount of data affected by the Client in connection with the case, due to their sensitivity

reported risks, as well as the market position of the Client, on the basis of which increased

it is expected to apply appropriate data security measures.

-

As reflected in its own internal policies, the Customer 's (open source) policy

the risks arising from the use of a content management system

must be borne and approved by the Client. The Customer on this

in the absence of such measures, it did not comply properly with its own internal rules.

-

Encryption applied to the personal data concerned and the risks involved

the lack of an assessment also increased the risks of exposure to the incident. On this

the application of the measure is also reflected in the relevant internal regulations of the Client,

which it also did not or did not fully comply with.

16

-

With respect to the digi.hu website, with administrator (administrator) rights

the Authority is seriously increasing the security risks

taken into account as a factor.

-

The Authority identified data security vulnerabilities at the system level

considers the problem that the infringement situation existed before the incident took place

also has existed for a long time with the data management Client regarding the affected databases.

-

In addition to data security vulnerabilities, the occurrence of the incident directly

traceable to the test database created for troubleshooting purposes is in principle infringing

for a long period […] in a way that is unintentional and identifiable

for storage. If the test database had been deleted in accordance with the principles

after the error correction goal has been achieved, it is reported to those affected by the incident

risks would also have been much milder, given the number of data subjects involved

could have been reduced by the number of people in the test database ([…] affected). The

data security deficiencies in case of timely deletion of the test database only the personal data managed in the direct

marketing database ([érintett] concerned) and the digi.hu website

administrator data ([…] concerned).

-

Identification of data processed without purpose, cleaning and updating of data

deletion as required is also included in Customer's internal regulations, which is also inconsistent

conditions for managing the test database involved in the incident.

-

There are a large number of data security vulnerabilities and breaches of data in principle

(a total of […] persons) affected the personal data of the data subject, which contains the Customer

retail customers […]. This is also significant in relation to the proportion of the country's population

number (population in Hungary […]).

-

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

Infringements of fundamental rights by Article 83 (5) of the General Data Protection Regulation

infringement falling within the higher maximum amount of the fine

are considered.

Mitigating circumstances:

-

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

personal data breach.

-

The Client also acknowledged in a statement that the test database involved in the incident has already been

you should have deleted it earlier.

Other circumstances considered:

-

Upon becoming aware of a privacy incident, Customer is the incident

Article 33 of the General Data Protection Regulation

took immediate action to investigate the incident before the Authority

within 72 hours of becoming aware of the vulnerability

has installed a patch and deleted the illegally managed database

in connection with the performance of vulnerability tests. The Authority is thus specific to the Client

did not reveal any problem in his privacy incident management practices. The Authority shall e

17

conduct, as it did not go beyond compliance with legal obligations

not assessed as an attenuating circumstance.

-

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

Authority in the investigation of the case, although this conduct is not - as the law

obligations were not exceeded either, he said

as a circumstance.

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

Publicly available financial statements for the year ended 31 January 2018 to 31 December 2018

Based on

in this

the

year

altogether

47,299,383,000

HUF

(forty-seven billion two hundred and ninety-nine million nine hundred and eighty-three thousand forints). The Authority

and took into account that the Customer's business between January 1, 2019 and December 31, 2019

year to the Authority NAIH / 2020/1160/6. reply to fact-finding order no

according to the net sales of HUF 51,890,528,182 (fifty-one billion eight hundred and ninety million five hundred and

twenty-eight hundred and eighty-two). Infringement in setting the fine

In view of the period of its existence, the Authority has taken into account the business years 2018 and 2019.

Based on the above, the amount of the fine imposed is proportionate to the gravity of the infringement.

The Authority shall inform Infotv. Pursuant to Section 61 (2) a) and c) of the decision, the Client

has also ordered the disclosure of your personal data (with the protection of business secrets),

whereas the infringement is serious and affects a wide range of persons.

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.

18

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

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

Decree

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

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

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

may request the court to adjudicate the emergency instead of adjudicating

postpone until the end of

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

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

el,

(c) no interim measure has been ordered.

The Ákr. According to § 132, if the debtor does not comply with the obligation contained in the final decision of the authority fulfilled, it is enforceable. The decision of the Authority With the communication pursuant to Section 82 (1) it becomes final. The Ákr. Section 133 of the Enforcement - if by law or government decree unless otherwise provided by the decision-making authority. The Ákr. Pursuant to § 134 a enforcement - if local in a law, government decree or municipal authority matter the decree of the local government does not provide otherwise - it is carried out by the state tax authority. Infotv. Pursuant to Section 60 (7), a specific act included in the decision of the Authority obligation to perform, specified conduct, tolerance or cessation the Authority shall enforce the decision.

Budapest, May 18, 2020

Dr. Attila Péterfalvi

President

c. professor