Case number:

Object:

NAIH / 2020/66/21

Clerk:

decision

ex officio

starting

privacy

official

procedure

DECISION

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

„ROBINSON-TOURS” Idegenforgalmi és Szolgáltató Kft. „F.a.” (registered office: 8230 Balatonfüred,

Gombás köz 5., company registration number: 19-09-501812) (hereinafter: Customer 1. or data controller)

(represented by: ECONO-GROUP Pénzügyi és Gazdasági Szakértő Kft., […] liquidator, address: 8200

Veszprém, Házgyári út 22 / B.) And the Next Time Media Agency Ltd. (registered office:

1202 Budapest, Fiume u. 17., company registration number: 01-09-294227) (hereinafter: Customer 2. or

on a data protection incident involving the processing of personal data on 30 January 2020

due to the circumstances revealed during the official inspection initiated on 2 April 2020

ex officio data protection authority proceedings

I. Customer 1. as a data controller

(1) finds that:

a) Customer 1. has not complied with the processing of personal data of natural persons

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

Regulation (EU) 2016/679 repealing Directive

Article 25 (1) to (2) of the General Data Protection Regulation)

the principle of default privacy, as the design of your website is not appropriate

entrusted a selected data controller, which is serious, in principle infringing and not

led to deficiencies in secure data management planning. The design, design

shortcomings directly allowed for the confidentiality of the data

high-risk privacy incident.

(b) Customer 1. has not complied with Article 32 (1) (b) of the General Data Protection Regulation

when it comes to the travel services it offers

used and stored its personal data storage system and website

operated to allow anyone to access the Internet through a vulnerability

because of its existence. Due to this shortcoming, the confidentiality of the data is severely compromised

damaged, which directly allowed the high-risk privacy incident

occurrence.

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

with the data protection incident that has occurred

when you did not report the high-risk privacy incident to

stakeholders.

2) instructs Client 1 to comply with this decision within 15 days of becoming final

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

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

3) due to the above violation, Customer 1 for 30 days from the date on which this decision became final

within

HUF 20,000,000, ie twenty million forints

order to pay a data protection fine;

II. Customer 2. as a data processor

1) finds that Customer 2. has not complied with Article 32 (1) of the General Data Protection Regulation;

paragraph (b) when anyone accesses the database affected by the incident

accessed through the Internet due to the existence of a vulnerability, so the data

the confidentiality of its processing has been seriously compromised. This is because Customer 2. is the website

did not break the link between the test and live databases concerned during its operation,

in addition, the website has not been subjected to proper security checks for vulnerabilities

tests. The omission directly allowed access to personal information and thus

the occurrence of a data protection incident.

2) due to the above violation, Customer 2 shall be granted 30 days from the date on which this decision becomes final

within

HUF 500,000, five hundred thousand forints

order to pay a data protection fine;

III. order the final decision by publishing Customer ID 1 and Customer ID 2

disclosure.

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

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

0425 0000 0000) must be paid by bank transfer. When transferring the amount, NAIH / 2020/66

JUDGE. number should be referred to.

The Customer took 1 to take the measures provided for in point I./2) from the time the measure was taken

You must provide proof in writing within 15 days, together with supporting evidence

to the Authority.

If Customer 1 and Customer 2 fail to comply with the obligation to pay the fine within the time limit

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

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

the Authority's centralized revenue collection forint account

(10032000-01040425-00000000 Centralized direct debit).

Failure to comply with the obligation under point I./2) and failure to pay the fine and the penalty for late payment

In the event of payment, the Authority shall order the enforcement of the decision, the fine and the penalty payment.

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

Within 30 days of the application addressed to the Metropolitan Court in an administrative lawsuit

2

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

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

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

acting outside. For those who do not benefit from full personal exemption, the administrative lawsuit

its fee is HUF 30,000, the lawsuit is subject to the right to record material fees. In the proceedings before the Metropolitan

Court a

legal representation is mandatory.

EXPLANATORY STATEMENT

I.

Background and clarification of the facts

1) On 29 December 2019, the Authority received a public interest notice calling on the

Please note that on the https://www.lastminute.robinsontours.hu/partnerkapu_ Occupations website

the personal data of the Customer's 1. natural person's customers are available to anyone through

such as passengers' names, contact details, address details, identity cards and

passport numbers, booking and travel, destination, accommodation and contracting

related data. The data is https://www.robinsontours.hu/partnerkapu_ Occupations link

were also available through. According to the announcement, the applicant realized this on the Internet

while browsing, type your father's name into Google's search engine and then one of the results

managed to open a database without any authorization check.

The Authority has verified the above links and NAIH / 2020/66/2., NAIH / 2020/66/3. and NAIH / 2020/66/5.

In its file number, he found that the links were in his web browser

entered, any authentication, or other IT security measures

As stated by the notifier, a

a database containing the personal data of various natural person customers. The

based on the data in the database, it is likely that most of them are as travel agents

Operating Customer 1. Customers using the travel services. The Authority is also satisfied that

that the data stored in the database is searched in a Google search engine (eg a passenger 's name)

search) can also be reached. So the content was also crawled by and in the Google search engine

made them available by keyword search.

The personal data available is as follows:

- name of 'guide',

- number and names of fellow travelers,

- date of departure and arrival, date of booking,

- reservation status (final / canceled / pending),

- reservation number,

- address details (country, postcode, town, street, house number, floor, door precision),

- identity card number with date of issue and expiry,

- passport number with date of issue and expiry,

- e-mail address, telephone number,

- date of conclusion of the travel contract.

On the website, it was also possible to filter people by destination and date. In the database of this

in addition, for each customer, anyone has the option to upload a passport photo or write a comment

next to each booking. By choosing to upload your passport photo, you can not only take pictures,

but virtually any file format could be selected for upload.

The table, which can be viewed via links, contained a total of 375 records. These were among them

are also likely to be fictitious persons (eg “TEST TEST”, “IVÁN TEST”, etc.), but

most of them covered existing natural person customers. Based on the number and names of fellow travelers

however, the data of many more than a thousand people were also available through the website.

From the database available through the links, it was also possible to connect with individual customers

travel contracts are free for anyone to download in pdf format. Of each contract

five copies have been downloaded as evidence by the acting administrator of the Authority, as well as an e-mail

certificate as well. The downloadable contracts were detailed in all contracted passengers

personal data, destination, date of travel, details of the accommodation booked and the gross amount of the service.

price broken down by person.

In view of the above, the Authority launched an official inspection on 30 January 2020, as a

the available data were not sufficient to conclude that Customer 1.

has fully complied with its obligations under the General Data Protection Regulation, thus

in particular 32-34. provided for in Article

2) In the later days (February 3, 2020), NAIH / 2020/66/7. with note no

according to a documented re-audit, the publicly available database is constantly being updated

records, including personal data and related contracts,

for uploading. The update of the customer database could thus be followed live on the website in this way

across. However, the database was no longer available in this way on 4 February 2020.

The Authority NAIH / 2020/66/4. by order no

Customer 1, which was received on February 4, 2020, as evidenced by the returned return receipt.

The Client 1. sent it together with the statement sent in time for the above order

a data protection incident report completed on the basis of a sample downloaded from the Authority's website.

Based on the incident report and the responses to the order, Customer 1. stated that the

the details of your customers who actually use your travel agency services via those links

were available. In addition to real individuals, they were included in the database for testing

also created fictitious persons. Customer 1. record the purpose of the data for each trip

identification of the data subject and the persons actually traveling

needs to be able to retrieve the agreements between the data subject and the 1. customer and a

you can contact stakeholders about performance. Only for the database

Representatives of partners contracted with Customer 1 were allowed to enter, with whom Customer 1 is valid had a contract.

The data in the database is 1. client on a dedicated server, structured, in SQL format stored. Client 1. Client 2 has been assigned as a data processor by the hosting provider, programmer, with administrator and IT service provider tasks. The data was stored on the Client's 2nd servers, the exact location of which is 1143 Budapest, Ilka u. Located in the Invitech server room under 31st. The data security in the interests of Customer 2. as a data processor the following measures implemented: firewall, anti-virus, multi-level authentication and access control, strong use and forced exchange of passwords, daily backup of the database, logging of data operations.

Client 1. stated that the Authority did not have NAIH / 2020/66/4. order no prior to receiving it, he was aware of the privacy incident as he was not notified of any business

its partners, nor its data processor or any other stakeholders, nor in the course of its own operations he noticed it. However, immediately upon becoming aware of the incident, it shall be investigated and Article 33 (1) of the General Data Protection Regulation has been notified to the Authority as Customer 1. after investigating the incident considered it to be at risk rights and freedoms of data subjects. Customer 1. The privacy incident is general also registered under Article 33 (5) of the Data Protection Regulation.

The cause of the incident was indicated by Customer 1 as a website operated by Customer 2 a test environment was created during development that was not removed from the final version. As a result, real, sharp data was also included in the data set used for testing.

This test environment, which is constantly updated with real data, has not been protected. Customer 1 he was unaware of this test environment, he did not even use it. As Customer's 1st website there was no direct reference to the test environment, so it is only available in could be reached by invoking a specific URL. Based on this, Customer 1. is likely to only

few had unauthorized access to the data.

Based on Customer Incident Report 1, the vulnerability is from November 13, 2019 to February 4, 2020

stood up through the website. The vulnerability affects a total of 781 people, for a total of approx. 2506 pieces

personal data, which are: name, address, date of birth, passport number and expiry date,

ID card number and expiration date, email address, phone number, departure and arrival

date and the details of each travel contract in pdf format (eg

contract value). The database involved in the incident also included data on minors. The

the personnel of the stakeholders at Customer 1 in the period from 13 November 2019 to 4 February 2020

It included Hungarian passengers and tour guides who booked trips.

Upon receipt of the Authority's order, Customer 1. immediately notified Customer 2 by telephone a

vulnerability, who immediately took steps to prevent the use of

to further achieve a test environment that is updated with live data. Customer's 1st assessment is

vulnerability that triggers a privacy incident overall Customer 2. not careful, careful

resulted from its procedure. Customer 1. further informed the Authority that the incident was due to regulatory

review its material. Customer 1. also stated that it plans to inform stakeholders a

the outcome of the official procedure after its conclusion.

3) The Authority's NAIH / 2020/66/10. to make further declarations and provide documents

called Customer 1, which was met by the deadline.

According to his replies, the contractors had access to the database affected by the incident

were travel agents signing a travel agency contract. A sample of the contract with them

Customer 1. attached to your reply. The database was accessed by a total of 307 travel agents who

however, they could not enter or modify data there. Each travel agent is only their own

he had access to his reservations. Only Customer 1. was entitled to enter data into the database.

Client 1. informed the Authority that there was no access to the database affected by the incident

an authorization control system has been set up, which has led to the occurrence of a data protection incident.

However, Customer 1. has since ordered the use of a username and password in the system, a

from now on, the database will only be accessible to authorized personnel.

Customer's policy on password management was described in the Customer's response.

5

Customer 1. explained that during the period of the vulnerability (November 13, 2019 -

February 4, 2020) 28 unauthorized accesses from a total of two IP addresses1

for a total of 30 documents, four times (30 and 31 January 2020 and 1 February

and days 3). A detectable privacy incident is thus actually associated with these occasions

materialized.

Customer 1. explained that the test environment created during development and the associated test database

- given that the testing was not done with sharp data - was not protected. At the end of testing

however, the data file was not deleted and remained associated with the separate, now sharp

system and database. Personal data entered by the Customer into the live system 1. a

they were also transferred to a test database as a data link remained between the two systems. THE

a constantly updated test database with live data was available through the vulnerability

(see figure below).

In the database available through the vulnerability for a total of 309 travel contracts

could be accessed. As previously described, these are a total of 781 affected, for a total of approx.

They contained 2506 pieces of personal information. A total of 46 of those affected were children (18

under one year).

The […] IP address identified by Customer 1 was determined by the Authority's acting administrator to be the IP address of the

Authority's Internet subscription. The database accesses that can be associated with this IP address are therefore subject to

official control

are most likely to be linked to queries documented in official records between

NAIH / 2020/66/13. s. recording).

1

6

Customer 1. also stated that the “upload passport copy” through the available interface

It was not possible to upload data from the outside via the option, as it was only uploaded to the live system

were able to upload Customer 1. staff in pdf or jpeg format. The sharp system

had virus protection.

Customer 1. Attached to the response to the Authority's call, the data processors with Customer 2

(‘data-processing agreement’, […]). He signed the contract on April 10, 2019

each other Customer 1 and Customer 2. According to clause 4 of the contract for the security of data processing

guarantee and take measures proportionate to the risks, as well as the data controller

support is the task and duty of the data processor (Customer 2). The task of the data processor is a

accidental or unlawful destruction or modification of personal data without permission

prevent their unauthorized access or unauthorized access.

To this end, it is required to take organizational and technical measures proportionate to the risks

to do. The data controller is obliged to have access to the data by unauthorized persons

damages resulting from willful or negligent breach of this obligation

responsibility. The data processor is obliged to constantly monitor the data

measures taken to comply with data protection law.

4) The Authority shall issue NAIH / 2020/66/12. to make further declarations and provide documents

called Customer 1, which was met by the deadline.

Attached to the response Customer 1. sent an unauthorized access detail statement

a table showing that 26 out of all document accesses

In this case, documents were downloaded from the Authority's IP address as part of an official control

(30 and 31 January 2020 and 1 and 3 February). The remaining four document accesses cannot be linked to the Authority's IP

address.

In addition to the above, the Customer has sent the “Complex IT System” concluded with the Customer 2

a copy of the contract dated 10 April 2019 on the development of

also the "data processing agreement" already referred to with that date. The contract

developed within the framework of this by Customer 2. to record travel bookings and
the system and database involved in the incident. The developed system and its
The purpose of the database was to be used by partners contracted with Customer 1
personal data of persons using intermediary travel services (identification data,
contact details, destination and travel details, contracts, documents, etc.)
be stored and handled.

5) In addition to further clarifying the facts, the case is covered by the General Data Protection Regulation
due to the necessary further investigation of the alleged breach of obligations by the Customer
Act CXII of 2011 on the right to information self-determination and freedom of information. Act (a
hereinafter: Infotv.), the Authority is included in the operative part
decided to initiate an official data protection procedure. The Authority was informed of this on 2 April 2020
NAIH / 2020/66/14. notified Customer 1 on 6 April 2020 by notifying the file number.

6) The Authority's NAIH / 2020/66/16. No. 2, dated 11 May 2020, notified Customer 2
to involve the general data protection authority in the data protection authority proceedings as a customer
due to an investigation into alleged breaches of the obligations under this Regulation
declaration and service of documents. Customer 2. responded to the order on time.

7

According to the Customer's 2nd statement, the test database affected by the incident - through which a
personal data has become available over the internet - in the meantime it has been deleted. The affected
In addition, Customer 2. has relocated the system to a more closed, secure system. This is the operation
it was still in progress at the time of the response.

Previously, "authentication checks" affecting system security based on Customer's Statement 2
they occurred only around the point of entry. The Authority's question is whether the scheme concerned
the frequency with which it is reviewed for security purposes, Customer 2. has only provided
that the protection of the website affected by the incident is fixed, otherwise “news from the web world and
whether the protection measures need to be updated.

To the Authority's question as to why the test version of the booking database behind the website is not previously deleted, Customer 2. replied that in his opinion the deletion did not makes sense because at some point you may need to ‘improve something’, ‘solve something’ so "Testing never ends". The interface between the test and the live database In connection with the termination of Customer 2. stated that in its opinion it is not it is an important issue because the (lack of) authorization check was the source of the error.

7) The Authority NAIH / 2020/66/19. by order no for the provision of documents to Customer 2, who responded to the order on time. Based on Customer's Statement 2, it does not currently have an IT Security Policy and Privacy Policy.

Customer 2. the system involved in the incident (the website), referred to by him as “authentication does not have a record, it has not documented them.

Customer 2. further stated that access to the database affected by the incident was unauthorized access log data is overwritten at 30-day intervals. By the time Customer 2. received the request (from Customer 1) that they are needed, only on January 24, 2020 - You were able to save your access log from February 10, 2020. This was sent by Customer 1, which was forwarded to the Authority by NAIH / 2020/66/12. to the previous order no attached to his reply. As a result, Client 1. informed the Authority that external accesses took place only on 30 and 31 January 2020 and on 1 and 3 February database.

8) The Authority's NAIH / 2020/66/18. invited Customer 1 to make a statement by order no. in which he requested, inter alia, a statement as to the size of the 2019 business year amount was the net sales revenue.

From the Customer's 1. registered office, the above order may be re-mailed twice Returned to the Authority with the word "not sought". The Authority is now in the register of companies Customer has been notified that the Customer is in liquidation as of June 16, 2020.

Customer 1. Data on its management in 2019 and 2020 will be published in the meantime

were posted on the Electronic Reporting Portal.

8

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.

Affected by a data protection 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) (f) of the General Data Protection Regulation, personal data

shall be handled in such a way that appropriate technical or organizational measures are taken

ensure the adequate security of personal data

unauthorized or unlawful handling, accidental loss, destruction or

including protection against damage ("integrity and confidentiality").

According to Article 25 (1) of the General Data Protection Regulation, the controller is a scientific and

the state of the art and the cost of implementation, as well as the nature and scope of data

the rights and freedoms of natural persons,

taking into account both the probability and severity of the risk and the way in which the data are handled

as well as the appropriate technical and organizational arrangements for data management

implement measures, such as pseudonymisation, aimed at complying with data protection principles,

such as the effective implementation of data saving, on the one hand, and the provisions of this Regulation, on the other

guarantees necessary to meet the requirements and to protect the rights of data subjects

integration into the data management process.

According to Article 25 (2) of the General Data Protection Regulation, the controller is technically appropriate

and implements organizational measures to ensure that by default

only personal data that is subject to that specific data processing should be processed

necessary for the purpose. This obligation applies to personal information collected

the extent of their handling, the duration of their storage and their availability. These are

measures in particular need to ensure that personal data is defaulted

cannot be accessed without the intervention of the natural person

for an indefinite number of persons.

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

the state of science and technology and the cost of implementation, and

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

taking into account the varying degrees of probability and severity of the

implement appropriate technical and organizational measures to address the risk

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

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

integrity, availability and resilience.

9

Security is adequate under Article 32 (2) of the General Data Protection Regulation

In determining the level of

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

accidental or unlawful destruction, loss, alteration, unauthorized

resulting from unauthorized disclosure of, or access to, them.

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

the controller without undue delay and, if possible, no later than 72 hours after
the data protection incident becomes known to the competent supervisory authority in accordance with Article 55
unless the data protection incident is not likely to pose a risk to the
the rights and freedoms of natural persons. If the notification is not made 72
within one hour, it shall be accompanied by the reasons for the delay. The data processor
without undue delay after becoming aware of the data protection incident
notifies the controller.
Pursuant to Article 34 (1) of the General Data Protection Regulation, if the data protection incident
is likely to pose a high risk to the rights and freedoms of natural persons
the data controller shall inform the data subject of the data protection without undue delay
incident.
Pursuant to Article 34 (4) of the General Data Protection Regulation, if the controller has not already done so
notified the data subject of the data protection incident, the supervisory authority, after considering that
whether the data protection incident is likely to involve a high risk, the data subject may order
one of the conditions referred to in paragraph 3
fulfillment.
Act CXII of 2011 on the right to information self-determination and freedom of information. law
(hereinafter: Infotv.) pursuant to Section 2 (2) of the General Data Protection Decree there
shall apply with the additions set out in the provisions set out in
The Ákr. Pursuant to Section 101 (1) (a), if the authority has committed an infringement during the official inspection
experience, initiates its official proceedings. Infotv. Section 38 (3) and Section 60 (1)
based on the Infotv. Personal data within the scope of its duties under Section 38 (2) and (2a)
ex officio in order to enforce the right to protection of personal data.
The Ákr. Pursuant to Section 103 (1) of the Act concerning the procedures initiated upon request
provisions of Art. It shall apply with the exceptions provided for in Sections 103 and 104.
Infotv. Pursuant to Section 61 (1) (a), the Authority shall comply with Section 2 (2) and (4)

in the context of certain data processing operations in the General Data Protection Regulation

may apply certain legal consequences.

Pursuant to Article 58 (2) (b) and (i) of the General Data Protection Regulation, the supervisory

the data controller or processor acting under the corrective powers of the competent authority if

breached the provisions of the Regulation or Article 83

impose an administrative fine accordingly, depending on the circumstances of the case

in addition to or instead of the measures referred to in Paragraph 2 of the same Article

In accordance with point (d), the supervisory authority, acting in its corrective capacity, shall instruct the controller

or the processor to carry out its data processing operations, where appropriate in a specified manner and

bring it into line with the provisions of this Regulation.

10

The conditions for the imposition of an administrative fine are set out in Article 83 of the General Data Protection Regulation.

contained in Article. In the event of a breach of Article 5 of the General Data Protection Regulation, it may be imposed

under Article 83 (5) (a) of the General Data Protection Regulation

000 000 (EUR) or, in the case of undertakings, the full financial year of the previous financial year

up to 4% of its worldwide turnover.

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

disclosure of the identity of the processor, if the

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

or the gravity of the infringement justifies disclosure.

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

III.

Decision

1. Management, high risk classification and reporting of a data protection incident

About the vulnerability that triggered the privacy incident, Customer 1. first said that a

Authority NAIH / 2020/66/4. obtained from a fact-finding order on 4 February 2020

note. He was previously unaware of the vulnerability and the privacy incident. Customer

1. access to a database containing data on data subjects using their travel services

access could not be detected by Client 1 itself, thus the incident and its enabler

only on the basis of an indication from the Authority.

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. The Authority shall grant several accesses on the basis of the information provided by the notifier in the public interest

created to the database through the vulnerability, and later Customer 1.

he also acknowledged the vulnerability in an incident report. Through a website maintained by Customer 1.

exploiting the available vulnerabilities, it was therefore possible to access the data concerned

access. Unauthorized access to personal information is therefore an IT security

This could have been the case in several cases

resulted. Of these unauthorized accesses, the Authority also identified several cases

documented in his cited notes.

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

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

data protection incident, he must report it to the supervisory authority. The incident

notification may be waived only if the incident is not likely to pose a risk to

the rights and freedoms of natural persons. Assessing the risks associated with the incident

the task of the data controller.

Recital 75 of the General Data Protection Regulation deals with the processing of data

which may result in identity theft or misuse of identity, and

in particular the processing of children's data in relation to the rights and freedoms of the persons concerned

considered fundamentally risky data management. The Authority also highlights that travel

from the data contained in the contracts, such as the time of the journey and the purpose of the contract

11

Further conclusions can also be drawn from the value of the passenger in relation to the financial circumstances of the given passenger. On this

in addition to the address data also available for the person concerned's stay at home

a conclusion can be drawn. The joint handling of this data compared to the incident

circumstances, the Authority considers that there is a high-risk data protection incident

resulted.

High risk to the privacy of the natural persons concerned

another important circumstance is that according to the statement of the Customer 2. (data processor) the data subject is concerned

External illegal access to the database shall be restricted to the period from 24 January 2020 to 10 February 2020.

he was able to save his diary. Total duration of the vulnerability (13 November 2019 -

The exact number of unauthorized accesses under February 4, 2020) is thus unknown.

based on the content of the public interest notification sent to the Authority on 29 December

has already been made, at least by the public interest notifier. The vulnerability lasts longer

its existence has also increased the risks.

In view of the above, the Authority also considers high risk to be a factor justifying

that the database was accessed by both the notifier in the public interest and the Authority, but that

the total number of unauthorized accesses and the identity of the accessors for the duration of the vulnerability

cannot be accurately measured in the absence of a complete log file for The identity of the accessors and

number 1. Customer can no longer subsequently assess and identify which is involved in the incident

gives a great deal of uncertainty and concern about the further fate of personal data

okot. The data controller is of an incalculable degree and scale, but has been proven to have happened

In the event of a data leak, you can only try to reduce the data subject by informing the data subject

high risks anyway.

The Authority considers that the additional circumstances justifying the high risk are that

The personal information processed in this database is also indexed by Google on this search engine

they were also accessible through them, making them much easier to access even on the internet

also when browsing, randomly searching for a name.

Based on the above, the Authority considers that the data protection incident is high risk

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 notification was made by the Data Controller by e-mail to the Authority on 6 February 2020,

having become aware of the Authority's decision of 4 February 2020

upon receipt. The data controller is thus obliged to report the incident

within 72 hours of receiving it. The Authority shall comply with the notification obligation

therefore found no infringement.

2. Informing data subjects about the data protection incident

In its 1st incident report, the client stated that it plans to inform the stakeholders a

the outcome of the official procedure after its conclusion. This statement or the official

on the basis of further statements sent to the Authority during the procedure, the Client 1. this decision

did not inform those concerned about the data protection incident by the general

under Article 34 of the Data Protection Regulation.

According to Article 34 (1) of the General Data Protection Regulation, it is the responsibility of the controller to:

inform data subjects of the data protection incident without undue delay, if any

considered a high-risk incident.

The Authority considers that the incident is of a high risk justifying

that, in accordance with Article 34 (1) of the General Data Protection Regulation, the data subject

as there may be spill-over effects on the privacy of data subjects

which the controller no longer has control over in the course of incident management which he may carry out

(see previous section III./1 of this Decision on risk classification).

Risks of the incident - in recitals 85 to 86 of the General Data Protection Regulation

can only be effectively mitigated if those concerned do so

they are aware and may take any further action they deem necessary.

Customer 1. as data controller is responsible for the occurrence of a data protection incident

you can assess your risks. This is because the data controller is primarily aware that

what personal data you handle, for what purposes and using data processing methods. The

the possible high risk classification of the data protection incident and therefore the information to the data subject

The main task of the Client is to assess the need for the assessment of this question

"Depending on the outcome of an official procedure" by referring to the supervisory authority. The

the controller shall inform the data subject of the incident without undue delay as soon as possible

has become known to him under Article 34 of the General Data Protection Regulation, he cannot wait for the authorities

until the end of the procedure.

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

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

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

which ensures similarly effective information to stakeholders.

Based on the above, the Authority finds that the Customer 1. in the absence or postponement of the information

did not comply with Article 34 (1) of the General Data Protection Regulation, therefore a

Pursuant to Article 34 (4), Client 1 requested that the parties concerned be informed

on the high-risk privacy incident.

3. Findings on security of data processing

The Authority also examined that Customer 1 as a data controller and Customer 2 as a data processor

the extent to which data security directly related to the incident has been complied with

requirements for an existing system.

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

and guaranteeing the data controller a level of data security commensurate with the degree of risk

technical and organizational measures in line with the state of science and technology

including personal data under Article 32 (1) (b) of the Regulation

the continuing confidentiality of the systems and services used to handle the data

integrity, availability and resilience.

This is confirmed by Article 32 (2) of the General Data Protection Regulation, which states that

in determining the appropriate level of security, the

risks arising from the processing of data, in particular those transmitted, stored or otherwise

accidental or unlawful destruction or loss of personal data

unauthorized disclosure or unauthorized disclosure

from access.

13

The vulnerability in the system affected by the data protection incident is therefore

inadequate security in the handling of personal data

settings were applied to the affected system as follows.

Customer 2. During the operation of the website, the connection between the test and live database involved

has not terminated, and the website has not been subject to adequate security or vulnerabilities

tests. The test database and already real data Customer 1. uploaded and used sharp

database thus maintained a connection channel through which the live data

were continuously transmitted in real time to the test database. This real-time connection

In addition to Customer's 1st and Customer's 2nd statements, trial downloads documented by the Authority and

accesses are also confirmed.

The vulnerability, a test database with live data, was available for this vulnerability

as its safety was no longer addressed by Customer 2. after the development was completed.

The incident would not have occurred if Customer had deleted the test database 2. or it was secure

relocates to the environment or disconnects from the live database. These are omissions

thus, personal data were made directly accessible.

The test database is essentially a vulnerable copy of the live database as defined above

functioned, the size of which increased steadily over time. This is customer data

will result in duplication for three months. Extremely for personal information

it was easily accessible from the outside without being noticed by Customer 1 or Customer 2.

Customer 1. processes personal data in connection with the travel services it offers

Due to the above, you have used and operated your storage system and website in a way that anyone can use

could access it over the Internet due to a vulnerability. This security

due to this deficiency, the confidentiality of the data is severely compromised, which is directly possible

made the high-risk privacy incident occur.

Customer 1. also referred to the fact that Customer 2. did not act as a data processor

quite carefully and carefully, and there was no authorization check for the system

system built.

In view of the above, the Authority concludes that:

- Customer 1. to load and manage data in the system, actually a

use of the system,

- Customer 2. careless operation and inadequate security control of the system and

through testing,

infringed Article 32 (1) (b) of the General Data Protection Regulation, as a

during the operation of the service, its confidentiality is neither data management nor data processing

could not guarantee.

4. Findings on the principle of privacy by design and default

Article 25 (1) to (2) of the General Data Protection Regulation contains the built-in and

default privacy

principle

according to which the risks of data management

appropriate technical and organizational measures must be taken by the controller

when determining the way in which data are to be processed, the purpose of which is to comply with data protection principles

effective implementation. In addition, the data controller is also responsible for providing appropriate technical and

implementation of organizational measures to ensure that only the specific purpose

necessary data management. These measures must, in particular, ensure that:

personal data by default without the intervention of a natural person

become accessible to an indefinite number of persons.

To the database involved in the incident, originally created for testing purposes (which will later be live

data is also constantly updated), via Google search and simple web links

held by anyone in the period from November 13, 2019 to February 4, 2020.

Managing the data stored in the database as explained in the previous sections alone

also resulted in high-risk data management, especially for children and contract

data. The handling of such data is therefore increasingly on the part of data controllers

technical and organizational measures proportionate to the high risk are expected

already in the planning period of data management in order to guarantee the principles of data management.

Guaranteeing the confidentiality of data processing is enshrined in Article 5 (1) of the General Data Protection Regulation.

also appears in paragraph (f). According to this, personal data must be processed in this way

to ensure that appropriate technical or organizational measures are taken

adequate security and confidentiality of personal data, such as illegal data processing

to prevent.

Pursuant to Article 25 (1) to (2), data controllers

they shall proceed in such a way that, at the start of the future processing, the

principles - e.g. the principles of integrity and confidentiality.

Customer 2. explained that in order to guarantee the confidentiality of the data management affected by the incident,

the entire system developed by him (which is practically Customer’s 1st website) during development

did not test, did not examine for safety, only performed “around the point of entry”

inspections, the error leading to the incident could not be detected earlier. Customer 2. and a

nor does it have records of the inspections carried out

could prove it. Within the framework of Client's 1st order, Client 2 therefore failed to perform the

website and system design and development during those security tests and other

measures to eliminate or eliminate the causes of the vulnerability

would have been (e.g. website vulnerability scan, test and live database remaining

disconnection of the test environment).

The lack of the above design measures allowed both knowing the link to the page to

both through Google’s search engine, anyone without any prior authorization checks

access personal data and documents stored on the online interface.

European Data Protection Board No. 4/2019, built-in and default data protection

The Guideline on the Principle of Data Protection states that data controllers already have new data processing

they must take into account the implementation of this principle and its implementation when planning it

they have to check and monitor later. The guidelines emphasize that

data controller is responsible for the principle of built-in and default data protection

data processing operations performed by the data controller (s) in order to fulfill their obligations

also in relation to. This must be taken into account by the controller when concluding a contract

with data processor.2

When defining data management, so in this case the website and related IT

the measures taken to design and develop the infrastructure were insufficient

in accordance with Article 25 of the General Data Protection Regulation

ensure their character. Due to this, later, through the website of personal information

they have become available to an indefinite number of people.

As the data controller, the Customer is responsible for the data processor entrusted by him (Customer 2).

due diligence must be taken into account when concluding a data-processing contract

act when selecting the appropriate data processor. Within the framework of the data processing contract

Customer 2. negligently designed and developed the system for which only the privacy

at the time of the incident, neither Customer 1 nor Customer 2 had previously obtained it

note.

At the basic level, data processing that is illegal, unsafe and leads to a serious incident is thus

was practically determined already in the design and development phase of the system, when even

specific data management has not yet started. Subsequent violations are straightforward

consequence of negligent design and improper data processing assignment.

Serious design deficiencies and non-compliance leading to a high-risk privacy incident

due to the order of the appropriate data processor Customer 1. therefore violated the general data protection

Article 25 (1) to (2) of this Regulation.

5. Sanction and justification applied

1) In clarifying the facts, the Authority has established with respect to Client 1 that the

data management

- infringed Article 25 (1) to (2) of the General Data Protection Regulation,

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

- infringed Article 34 (1) of the General Data Protection Regulation.

In view of this, the Authority instructed the Client to do so in accordance with the provisions of the operative part

take the necessary measures to inform those concerned about the data protection incident

Article 34 of the General Data Protection Regulation.

The Authority has examined whether it is justified to impose a data protection fine on Customer 1. E

Article 83 (2) of the GDPR and Infotv. 75 / A. § considered by the

all the circumstances of the case.

In view of this, the Authority Pursuant to Section 61 (1) (a), in the operative part

also decided to pay a data protection fine in the present decision

obliged.

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

2https: //edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

The Authority considered the following as an aggravating circumstance:

-

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

therefore, data controllers should exercise extreme caution

to ensure a level of data security appropriate to the degree of risk. Customer 1.

nevertheless, a large number of personal data (a total of 781 data subjects, a total of about 2506 pieces)

personal data, including data on children and contractual amounts

ensure the continued confidentiality of the system used to handle the data

has not taken appropriate measures to

-

The Authority found that a fundamentally high-risk data management

Customer 1. Unsuitable for preventing and detecting unauthorized access, a

applied disproportionate data security measures when personal

data was extremely easily accessible from the outside without being noticed by Customer 1.

would be. Security preparedness to handle such data from for-profit businesses

highly expected.

-

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

No privacy incident was detected by Customer 1.

-

The Authority identified identified data security vulnerabilities as a systemic problem

considers that the infringing situation is already the evidence of unauthorized access

the relevant test database existed at the data controller months before the occurrence

respect.

-

The breach of data confidentiality was practically determined by the system

sloppy design when specific data management has not even begun. The later

infringing data processing is a direct consequence of negligent design and inadequate

data processing mandate.

-

Customer 1. as a data controller is responsible for ensuring that any data protection occurs

assess the risks of an incident. This is because the data controller is aware that

what personal data, for what purposes and using data processing methods

treats. The potential high risk classification of a privacy incident and therefore about

Assessing the need for information about the customer The main task of the Customer is this issue

reference to the “functions of the outcome of an official procedure” a

supervisory authority. The controller shall, without undue delay, consult the data subject

report the incident as soon as it becomes aware of it under Article 34 of the General Data Protection Regulation.

may not wait until the formal procedure has been completed.

The Authority considered the following as mitigating circumstances:

-

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

that the persons concerned have suffered damage as a result of the infringement.

-

From the facts revealed, it can be concluded that the infringement was not intentional

Caused by customer 1. negligence. This is also indicated by the fact that the Client is about the incident

immediately after becoming aware of the vulnerability, the detected vulnerability was taken

in order to eliminate.

17

-

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

personal data breach.

Other circumstances considered:

-

Upon becoming aware of a privacy incident, Customer 1. is the incident

Article 33 of the General Data Protection Regulation

took immediate action to investigate the incident before the Authority

reported the vulnerability within 72 hours of becoming aware of it, Customer 2.

terminated and unlawfully managed the database. The Authority

Thus, Customer 1 did not identify any issues with its specific privacy incident management practices.

The Authority did not go beyond what was required to comply with its legal obligations.

did not assess it as an express mitigating circumstance.

-

The Authority also took into account that Customer 1. cooperated in all matters a

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 view of the above, the Authority considers it necessary to impose a fine, only the Infotv. 75 / A.

Did not consider it appropriate to apply the warning under

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

determined.

Infringements by Customer 1. Article 83 (4) (a) of the General Data Protection Regulation

are considered to be an infringement of the lower fine category.

In imposing the fine, the Authority finally took into account the economic weight of the Client. In this circle

took into account that

- 2019.

year

report

according to

5,344,545,000

HUF

(five billion three hundred and forty-four million to five hundred and forty-five thousand forints).

- According to its annual report closing the liquidation activity for 2020, on 1 January 2020

In the period between 2015 and June 15, 2020, it had net sales of HUF 551,404,000 (HUF five hundred and fifty-one million four hundred and four thousand).

- It will be liquidated from 16 June 2020.

The Authority for the period of the infringement (13 November 2019 to 4 February 2020)

took into account the economic data for 2019 and 2020. The infringement

In view of the weight of the Company and the above-mentioned management data of the Client, the amount of the fine imposed is therefore a

In the opinion of the Authority, it can be considered proportionate to the gravity of the infringement.

2) In clarifying the facts, the Authority has established with regard to Client 2 that the

infringed Article 32 (1) of the General Data Protection Regulation in the processing of

(b).

The Authority has examined whether it is justified to impose a data protection fine on Customer 2.

In this context, the Authority will amend Article 83 (2) of the GDPR and Infotv. 75 / A. § considered by the

all the circumstances of the case.

18

In view of this, the Authority Pursuant to Section 61 (1) (a), in the operative part

and in this decision the Customer 2 to pay a data protection fine

obliged.

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

The Authority considered the following as an aggravating circumstance:

-

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

therefore data controllers should exercise extreme caution

to ensure a level of data security appropriate to the degree of risk. Customer 2.

nevertheless, a large number of personal data (a total of 781 data subjects, a total of about 2506 pieces)

personal data, including data on children and contractual amounts

system) developed and operated by the Customer for the management of data

has not taken appropriate measures to ensure its continued confidentiality.

-

The Authority found that a fundamentally high-risk data management

Customer 2. Unsuitable for the prevention and detection of unauthorized access, a

applied disproportionate data security measures when personal

data was extremely easily accessible from the outside without being noticed by Customer 2.

would be. Security preparedness to handle such data from for-profit businesses

highly expected.

-

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

No privacy incident was detected by Customer 2.

-

The Authority identified identified data security vulnerabilities as a systemic problem

considers that the infringing situation is already the evidence of unauthorized access

months before the occurrence of the test database in question.

-

Customer 2. failed to perform the security of the website and system development

tests or other security measures to detect the vulnerability; or

could have been eliminated (e.g. website vulnerability scan, test and live database

termination of the remaining relationship). These defaults to Customer 2 are high

as the main activity is the provision of IT services

operates as a business.

The Authority took into account as mitigating circumstances:

-

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

that the persons concerned have suffered damage as a result of the infringement.

-

The Authority took into account that Client 2 had not previously established a

personal data breach.

Other circumstances considered:

-

The Authority also took into account that Customer 2. cooperated in all matters a

Authority during the investigation of the case, although this conduct - as required by law

obligations were also not exceeded - it was not assessed as explicitly mitigating

as a circumstance.

In view of the above, the Authority considers it necessary to impose a fine, only the Infotv. 75 / A.

Did not consider it appropriate to apply the warning under

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

determined.

Infringements by Customer 2. Article 83 (4) (a) of the General Data Protection Regulation

are considered to be an infringement of the lower fine category.

In imposing the fine, the Authority finally took into account the economic weight of the Client. In this circle

took into account that

- According to its report for 2019, HUF 47,155,000 (forty-seven million to one hundred and fifty-five thousand forints)

had net sales.

- According to its annual report for the year 2020 due to the changeover of the tax type, the financial statements for the year

ended 1 January 2020

and in the period from 31 March 2020 to HUF 1,772,000 (one million seven hundred and seventy-two thousand

HUF) net sales.

The Authority for the period of the infringement (13 November 2019 to 4 February 2020)

took into account the economic data for 2019 and 2020. The infringement

The amount of the fine imposed is therefore a

In the opinion of the Authority, it can be considered proportionate to the gravity of the infringement.

3) The Authority shall issue the Infotv. Pursuant to Section 61 (2) (a) and (c), the Customer shall

Customer 2 was also ordered to disclose his credentials because of the violation

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 (1) by decision of the Authority

The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (3) a)

Pursuant to point (aa) of the Act, the Metropolitan Court has exclusive jurisdiction. A Kp. Section 27 (1)

(b), legal representation is mandatory in litigation falling within the jurisdiction of the Tribunal. A Kp. § 39

(6) of the application for the entry into force of the administrative act

has no suspensive effect.

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

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

hereinafter referred to as the Customer's legal representative pursuant to Section 9 (1) (b) of the E-Administration Act

obliged to communicate electronically.

20

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

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

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

Fees. law

(hereinafter: Itv.) 45 / A. § (1). From the advance payment of the fee is

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

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

According to Section 35 of the Government Decree (hereinafter: the 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, December 9, 2020

Dr. Attila Péterfalvi

President

c. professor