Case number: NAIH / 2019/1841

History case number: NAIH / 2018/6093 / H

Subject: Partial decision granting the application

DECISION

Before the National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority) […]

hereinafter referred to as the "Applicant") was brought against […] (hereinafter referred to as the "Applicant")

take the following decisions in the data protection authority procedure:

I. The part of the Application relating to the finding of unlawful data processing

space and

I.1. notes that the Applicant did not facilitate the exercise of the Applicant's rights as a data subject.

I.2. notes that the Applicant has assessed the Applicant's request for cancellation and the application

did not comply with the transparency requirement when informing them of the measures taken.

II. It requests the Applicant to do so within 30 days of receipt of the decision

inform the Applicant to delete backups containing your personal data

and the conditions for using the backups. The information

also to the Authority.

III. Condemns the Applicant and

HUF 500,000, ie five hundred thousand forints

data protection fine

obliges to pay.

The fine was centralized by the Authority within 15 days of the decision becoming final

Receipt of receivables target settlement forint account (10032000-01040425-00000000 Centralized

collection account IBAN: HU83 1003 2000 0104 0425 0000 0000). The amount

NAIH / 2019/1841 / H. JUDGE. number should be referred to.

If the Debtor fails to meet its obligation to pay the fine within the time limit, the above

is required to pay a late payment surcharge on the account number. The amount of the late payment allowance is every

calendar day

365th of twice the central bank base rate in force at the time of the charge. THE

in the event of non-payment of a fine and a late payment allowance, the Authority shall order the decision

recovery of fines and penalties for late payment. The fine and the

the National Tax and Customs Administration collects the late payment surcharge.

2

ARC. The part of the application seeking an order from the Authority to delete his personal data a

He rejects the applicant.

V. Dismisses the part of the application concerning the publication of the decision and the imposition of the fine;

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

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

the application shall be submitted to the Authority, by electronic means, which shall forward it together with the file

to the court. The request for a hearing must be indicated in the application. The whole personal

for those who do not benefit from an exemption, the fee for the court review procedure is HUF 30,000;

subject to the right to record material duty. Legal representation is mandatory in proceedings before the Metropolitan Court.

EXPLANATORY STATEMENT

I. Procedure and clarification of the facts

In its application received by the Authority on 27 September 2018, the Applicant submitted that […]

He assigned to the applicant a claim against him which expired in 2011.

On 16 July 2018, the Applicant called on the Applicant to perform. The Applicant a

Upon receipt of his letter from the applicant, he contacted him to clarify the matter

with both […]. and the Applicant because he did not consider the claim to be justified.

The Applicant disputed the data management of the Applicant in an e-mail written to the Applicant

and requested that the Applicant make it available to him

documents on which the Applicant based his claim or requested information from the

From the applicant about the personal data he handles.

The Applicant asked the Applicant to identify him with his natural identity data

himself, as this is the only way to comply with his application, but this was refused by the Applicant because

in its view, the case number and name are sufficient to identify it. Thereafter, the Applicant

again by e-mail requesting the Applicant to mail the previously requested documents

sent to him by road and asked the Applicant to delete his e-mail address.

The Applicant informed the Applicant by e-mail that it had not been successful

therefore close the procedure for investigating your complaint. Thereafter, the Applicant

requested the deletion of your personal data by mail. In the Mail received by the Requested Return Receipt

informed that the […]. repurchased the claim and for the deletion of the Applicant's personal data

but your personal data can still be found in your IT system

backups, however, will repeatedly take action to delete them if the backups

or, failing that, permanently together with the backups

will be deleted in accordance with the Requested Backup Policy.

In the Applicant's view, it is not sufficient for the Applicant to take action on his personal data

but must fully implement it and inform it of its implementation.

He further complained that he had not informed the Applicant about the use of the backups,

it also finds it prejudicial that the Applicant is subject to the provisions of the Accounting Act

Pursuant to Act C of 2000 (hereinafter: the Act), the assignment intends to manage for eight years

documents received in the framework of the management of claims and subsequently created in the course of debt

management, which contain the

personal information. He further complained that during the identification by e-mail the Applicant

requested the provision of all natural personally identifiable information. In its view, the

The applicant unlawfully refused his request for access and did not cancel it despite his request

your email address.

The Applicant is required to establish the above violations and to delete the Applicant's personal data

the imposition of a fine in the public interest against the Applicant and the conviction

requested the Authority to publish a decision

At the request of the Applicant, on the right to self-determination of information and freedom of information

2011 CXII. Pursuant to Section 60 (1) of the Act (hereinafter: the Information Act), NAIH / 2018/6093 / H.

proceedings were initiated by a data protection authority.

I.1.2. In its order, the Authority requested information on the matter from the Applicant

in order to clarify.

The Applicant has informed the Authority that the personal data of the Applicant have been

deleted assigned receivables from its registration system. In support of this, he attached

Case 834950000831 from the assigned receivables registration system

screenshot. The case number could only be linked to the Applicant because the Applicant had previously

has lodged a complaint in connection with the Applicant 's proceedings, therefore the

Applicant was identifiable.

The Requested has been supported by screenshots to substantiate the complaint handling

the name of the Applicant, the case identifier and the data related to his / her complaint

(date of receipt of the complaint, method of lodging the complaint, justification of the Applicant's reply,

date of dispatch, brief description of the complaint, reason for the resolution, designation of the assignor,

complaint identifier) are included. This data is requested by the Applicant for general privacy

pursuant to its legal obligation under Article 6 (1) (c) of this Regulation.

According to the Applicant's statement, for its continuous operation and recoverability

In view of the requirement, the Applicant has a legal obligation to the assignee

the system for recording claims and all expenses incurred in the course of its activities

back up your data. The backup copies shall be made available to the Data Processor of the Requested,

[…] Performs. The Requested will have access to the backups in the event of a restore

necessary, for example due to a data loss incident. The obligation to make a backup

financial institutions, insurance undertakings and reinsurance undertakings for the Applicant, and

on the protection of the IT systems of investment firms and commodity exchange service providers

42/2015. (III. 12.) Government Decree (hereinafter: the IT Regulations of Financial Institutions)

Government Decree on the Protection of the System) 5 / B. § d).

The “Backup and restore operational procedure” policy for the requested restore

according to each save for 31 days, the last full save of the month for 12 months, the last full of the year

and its saving will be kept for 10 years.

4

Access to backups is restricted, with only certain privileges

have access to. Restore backups older than 30 days

may be requested from […] only upon reasoned request.

The Candidate attached to its response the Data Management Manual Customer Inquiry

(hereinafter referred to as the "Data Management Report")

manual), which contains the identification procedure and the complaint handling register

A screenshot of the applicant's entries.

II. Applicable legal provisions

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on natural

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

free movement of goods and repealing Regulation (EC) No 95/46 (general

under Article 2 (1) of the Data Protection Regulation) ('the GDPR')

the GDPR shall apply to data processing.

The relevant provisions of the GDPR in the present case are the following:

Recital 39: The processing of personal data must be lawful and fair

be. It must be transparent to natural persons that it applies to them

how their personal information is collected, used, viewed or otherwise

and the extent to which personal data are processed

are being treated or will be treated. The principle of transparency requires that personal data be processed

related information and communication is easily accessible and comprehensible,

and that it is worded clearly and in plain language. This principle applies

in particular to inform data subjects of the identity of the controller and the purpose of the processing,

and further information to ensure the protection of the data subject's personal data

fair and transparent treatment and the provision of information to data subjects

confirmation and information about the data processed about them. The natural person is the personal

information about the risks, rules, guarantees and rights associated with the processing of data

and how you can exercise your data management rights. THE

the specific purposes of the processing of personal data, in particular those explicitly stated, and

already established at the time of collection of the personal data

they must be. Personal data must be suitable and relevant for the purpose for which it is processed

and the scope of the data should be limited to the minimum necessary for the purpose. And for that

in particular, it must be ensured that personal data are stored for the shortest possible period of time

be limited. Personal data may only be processed if the purpose of the processing is different

cannot be reasonably achieved by the device. To ensure that it is personal

data storage is limited to the time required by the data controller for deletion or regular

review deadlines. Correction or deletion of inaccurate personal information

all reasonable steps must be taken to ensure that Personal data must be processed in a way that

which ensures their adequate level of security and confidentiality, including its

in order to prevent personal data and the processing of personal data

unauthorized access to or use of the devices used.

GDPR Recital 64: The controller shall take all reasonable measures to a

to identify the data subject requesting access, in particular online

services and online IDs. The data controller may not retain the

personal data for the sole purpose of responding to possible requests.

GDPR Article 5 (1) (a) and (b): Personal data:

(a) be processed lawfully and fairly and in a manner which is transparent to the data subject

("legality, fairness and transparency");

(c) be appropriate and relevant to the purposes for which the data are processed; and

should be limited to what is necessary ("data saving").

GDPR Article 6 (1) (c): Processing of personal data only if and to the extent that

lawful if at least one of the following is met:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject.

Article 6 (3) GDPR: The legal basis for the processing under paragraph 1 (c) and (e) is

shall state:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

Article 12 (2) GDPR: The controller shall facilitate the of its rights under Article

exercise. In the cases referred to in Article 11 (2), the controller shall article

You may not refuse to comply with your request to exercise your rights under this Article unless

proves that the data subject cannot be identified.

GDPR Article 12 (4): If the controller does not take action on the data subject's request

without delay, but no later than one month after receipt of the request

inform the data subject of the reasons for not taking action and that he or she is concerned

you can lodge a complaint with a supervisory authority and have the right to a judicial remedy.

Article 12 (6) GDPR: Without prejudice to Article 11, if the controller has reasonable doubts

are 15-21. the identity of the natural person submitting the application under Article

providing additional information necessary to confirm the identity of the data subject

you can ask.

Article 15 (1) GDPR: The data subject has the right to receive feedback from the controller

whether and where the processing of your personal data is in progress

is entitled to access personal data and the following information

get access to:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients with whom the personal data are held

have been or will be communicated, including in particular to third country consignees, and

international organizations;

(d) where applicable, the intended period for which the personal data will be stored or, if that is not possible,

criteria for determining this period;

(e) the data subject's right to request personal data concerning him or her from the controller

rectification, erasure or restriction on the processing of such personal data

against its treatment;

(f) the right to lodge a complaint with a supervisory authority;

(g) if the data were not collected from the data subject, all available information on their source;

(h) the fact of automated decision-making referred to in Article 22 (1) and (4), including:

profiling and, at least in these cases, the logic used

understandable information about the significance of such data processing and what it is for the data subject

with expected consequences.

Article 15 (3) GDPR: The controller is the personal data which are the subject of the processing

make a copy available to the data subject. For further copies requested by the data subject,

the controller may charge a reasonable fee based on administrative costs. If that

submitted the application electronically, the information was widely used

shall be provided in electronic format, unless otherwise requested by the data subject.

Article 17 (1) GDPR: The data subject has the right to request that the controller is unjustified

delete personal data concerning him without delay and the controller shall:

delete the personal data of the data subject without undue delay if the following

for one of the following reasons:

(a) personal data are no longer required for the purpose for which they were collected or for other purposes

treated;

(b) the data subject withdraws the authorization provided for in Article 6 (1) (a) or Article 9 (2) (a);

consent to the processing, and there is no other consent to the processing

legal basis;

(d) personal data have been processed unlawfully.

GDPR Article 17 (3) (b): Paragraphs 1 and 2 shall not apply if

data management required:

(b) the Union or Member State law applicable to the controller governing the processing of personal data

or in the public interest or in the exercise of official authority vested in the controller

to perform a task performed in the exercise of a license;

Article 58 (2) (b) to (c) and (i) GDPR: Acting in the corrective power of the supervisory authority:

(b) condemn the controller or the processor if he or she has breached his or her data processing activities

the provisions of this Regulation;

(c) instruct the controller or processor to comply with the conditions laid down in this Regulation

request for the exercise of his rights;

(i) impose an administrative fine in accordance with Article 83, depending on the circumstances of the case

in addition to or instead of the measures referred to in this paragraph.

Article 83 (1) to (2) and (5) (a) to (b) of the GDPR: 1. Each supervisory authority shall ensure that:

infringements of this Regulation referred to in paragraphs 4, 5 and 6

administrative fines shall be effective, proportionate and dissuasive in each case

be.

2. Administrative fines shall be imposed in accordance with Article 58 (2), depending on the circumstances of the case

It shall be imposed in addition to or instead of the measures referred to in points (a) to (h) and (j). When deciding

whether it is necessary to impose an administrative fine or the amount of the administrative fine

In each case, due account shall be taken of the following:

7

(a) the nature, gravity and duration of the breach, taking into account the processing in question

the nature, scope or purpose of the infringement and the number of persons affected by and affected by the infringement

the extent of the damage suffered;

(b) the intentional or negligent nature of the infringement;

(c) the mitigation of damage caused to the data subject by the controller or the processor

any measures taken to

(d) the extent of the responsibility of the controller or processor, taking into account the

and the technical and organizational measures taken pursuant to Article 32;

(e) relevant infringements previously committed by the controller or processor;

(f) the supervisory authority to remedy the breach and the possible negative effects of the breach

the degree of cooperation to alleviate

(g) the categories of personal data concerned by the breach;

(h) the manner in which the supervisory authority became aware of the infringement, in particular that:

whether the breach was reported by the controller or processor and, if so, what

in detail;

(i) if previously against the controller or processor concerned, on the same subject matter

- has ordered one of the measures referred to in Article 58 (2), the person in question

compliance with measures;

(j) whether the controller or processor has kept itself approved in accordance with Article 40

codes of conduct or approved certification mechanisms in accordance with Article 42;

and

(k) other aggravating or mitigating factors relevant to the circumstances of the case, such as:

financial gain or avoidance as a direct or indirect consequence of the infringement

loss.

5. Infringements of the following provisions in accordance with paragraph 2 shall not exceed 20 000 000

With an administrative fine of EUR 1 million or, in the case of undertakings, the previous financial year in full

up to 4% of its annual worldwide turnover,

the higher amount shall be charged:

(a) the principles of data processing, including the conditions for consent, in accordance with Articles 5, 6, 7 and 9;

(b) the rights of data subjects under Articles 12 to 22. in accordance with Article

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

shall apply with the additions provided for in

Infotv. Pursuant to Section 5 (3), Article 6 (1) (c) and (e) of the General Data Protection Regulation

in the case of data management specified in point (hereinafter: mandatory data management)

the types of data, the purpose and conditions of the data processing, the availability of the data, the

the duration of the processing or the periodic review of its necessity

defined by a law or a municipal decree ordering data processing.

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

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

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

rules shall apply with the additions specified in the Infotv. and the general data protection

with derogations under this Regulation.

8

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

by the activities of a body performing a public task

or the gravity of the infringement justifies disclosure.

Infotv. 75 / A. §, the Authority shall comply with Article 83 (2) to (6) of the General Data Protection Regulation

shall exercise its powers in accordance with the principle of proportionality, in particular by:

legislation on the processing of personal data or binding European Union law

for the first time in the event of a breach of the rules laid down in

in accordance with Article 58 of the General Data Protection Regulation

by alerting the controller or processor.

Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings Act (a

hereinafter: Hpt.) 67 / A. § (1): The activity of financial service providers - the ancillary

with the exception of financial services, using only an IT system

can take place, which ensures the closure of system components and prevents IT

unauthorized access to the system and unauthorized modification. IT

the system must also comply with the general information security confidentiality requirements.

To this end, the credit institution must provide administrative, physical and logical arrangements

compliance with the general information security confidentiality requirements.

Hpt. Section 288 (3): The financial institution and the independent intermediary shall file and file a complaint

shall keep the answer for five years and present it at the request of the Supervision.

Sztv. Section 166 (1): An accounting document is any such document issued, prepared, prepared by the enterprise.

or a natural person or other person with a business or other relationship with the enterprise

a document issued by the farmer (invoice, contract, agreement, statement,

credit institution statement, bank statement, legal provision, other documents that can be classified as such), regardless of the

printing or other method of production - which

supports its accounting.

Sztv. Section 169 (2): Directly and indirectly supports the accounting

accounting document (including general ledger accounts, analytical and detailed

records) must be in a legible form for at least 8 years, with reference to the accounting records

retained in a traceable manner.

Investment firms, payment institutions, electronic money issuers

institutions, issuers of vouchers, financial institutions and independent financial services

related to the complaint handling procedure of intermediaries and the complaint handling policy

435/2016 on detailed rules. (XII. 16.) Government Decree (hereinafter: Complaint Management

Government Decree) Section 3 (2) - (3): The service provider shall inform the customer about the complaints

keep records of the measures taken to settle and resolve

(3) It shall be included in the register referred to in paragraph 2

a) a description of the complaint, an indication of the event or fact which is the subject of the complaint,

b) the date on which the complaint was lodged,

(c) a description of the action taken to settle or resolve the complaint, if any

the reason

9

(d) the time limit for completion of the measure referred to in point (c) and the person responsible for its implementation

and

(e) the date on which the complaint was answered.

Financial institutions, insurance and reinsurance undertakings, investment firms and

42/2015 on the protection of the IT system of commodity exchange service providers. (III. 12.) Korm.

Regulation 5 / B. § d): The IT system complies with Hpt. 67 / A. § (1), the Bszt.

§ 12 (12) - (14), the Fsztv. 12 / A. § and the Bit. Section 94 (4) - (6), a

unauthorized access to the IT system and

unnoticed

amendment

by preventing

related,

and

the

general

information security confidentiality requirements if

(d) the data backup and recovery arrangements of the live system ensure that the system is secure

and restore-restore with the frequency and

documented tested.

CL of 2016 on General Administrative Procedure. Section 10 (1) of the Act (hereinafter: the Act)

customer is the natural or legal person or other entity to which

his right or legitimate interest is directly affected by the matter for which the official register is held

contains data or who has been placed under official control.

The Ákr. Pursuant to Section 35 (1), the application is a statement by the client by which it is an official procedure

enforcement of his right or legitimate interest

in order to.

III. Decision:

III.1. Facilitating the exercise of the Applicant's rights

III.1.1. Identification of the Applicant

In the Data Management Manual, the Applicant distinguishes between identification and identification

between cases that do not require it.

The Data Management Manual 3.1. (a), 'provided that the letter sent by post contains

(content, case identification, signature, etc.) is entitled to act in respect of the given claim

sent by the person (Customer himself, his agent, etc.), identification shall not apply. "

Section 3.2 of the Applicant's Data Management Manual. in a particular case

an e-mail is received from a previously unrecorded e-mail address, in which case it is necessary to

natural person with the natural identity data of the customer (name, place and time of birth, mother

name). In the case of the Applicant's complaint, the Applicant shall also comply with the Data Management

acted in accordance with the provisions of the Handbook, ie as before - on the transfer register

- did not know the Applicant's e-mail address, so his application

in order to meet its feasibility, it called on the Applicant to identify itself as natural

with your personal information.

The difference between cases requiring identification and those not requiring identification is that in the latter case a request contains additional information that ensures the identification of the sending party.

10

Such additional data content is contained in a letter sent by post that contains the sending party signature and home address or mailing address as opposed to a traditional e-mail or if the e-mail address was included in the data received from the transferor.

In the light of the above, it is not disputed that the Applicant must in any way identify the senders of letters from e-mail addresses whose identity is indeed well-founded.

up. However, proof of identity and identification are not the same concepts, so is

only all natural personal data are required for identification in exceptional cases

In most cases, the name and three additional personal details are sufficient

one if it is actually necessary to identify the customer. This, of course, does not close

who is identified by a name and customer number or a combination of name, customer number and home address

sem. The Applicant must investigate on a case-by-case basis the identity of the specific person sending the e-mail

whether there is a well-founded doubt under Article 12 (6) of the GDPR and

exactly which personal data - exceptionally personal data - you have to provide

need.

The e-mail sent by the Applicant did not contain any additional personal data other than the name,

from which the Applicant could have ascertained the identity of the Applicant, as by the Applicant

The given case number is used primarily to identify the case and not the customer. That's why it is

it cannot be objected that the Applicant has requested additional personal data from the Applicant,

however, it should have considered whether all four were necessary to identify the Applicant

natural identity data. The Applicant did not carry out this assessment, it is supported

the following:

The Applicant is attached by the employee who deletes the Applicant's personal data

a statement that “the claim registered under file number 834950000831 by me
has been anonymised, ie personal data has been deleted from the case, personal
data has been replaced by XXX. " Register of claims assigned by the Applicant
on the screen saver for claim 834950000831 a
Applicant's date of birth field is empty and does not contain XXX. It follows from the above that
that the Applicant has not been processed by the Applicant prior to the deletion of the Applicant's personal data
date of birth. For this reason, the Applicant requested the provision of such personal data a
Applicant in order to identify what he did not have to compare, from which he could not
would have ascertained the identity of the Applicant, so the Applicant’s date of birth was not
suitable for the identification of the Applicant by the Applicant. Because the Applicant did not provide
in order to identify the date of birth, therefore no unlawful data processing has taken place.
In view of the above, the Authority concludes that the application of Article 5 (1) (c) of the GDPR
however, the risk of a breach of the principle of data protection existed when the Applicant
requested the Applicant to provide his date of birth in order to:
did not have the Applicant's date of birth at the time of the summons, imposing an illegal condition
the fulfillment of the Applicant's requests for the exercise of the rights concerned.
III.1.2. The Data Management Manual 3.1. (a), 'provided that the letter sent by post is
to act on the basis of its contents (content, case identification, signature, etc.) with regard to the given claim
sent by an authorized person (the Customer himself, his agent, etc.), so no identification
applicable."
11
By letter dated 13 August 2018, the Applicant refused to be natural
identify yourself with your personally identifiable request or complaint in the email
in order to assess. By letter dated 14 August 2018, the Applicant informed the a
Applicant that, in the absence of identification, will close his complaint investigation procedure, however
did not provide him with information that he could request an inquiry into his complaint by post, and

request for additional natural personal data submitted in this form

in the absence of it, if it contains his name, case number and signature.

As a result, the Applicant did not facilitate the Applicant's ability to exercise his rights as a data subject,

he did not inform about the further possibilities of legal enforcement of the data subject, and even the complaint handling

procedure

in breach of Article 12 (2) of the GDPR.

III.2. Request by the Applicant to exercise the right of access

By e-mail dated 21 July 2018, the Applicant requested the Applicant to provide it

documents supporting the validity of the Claimant's claim,

and provide information on the legislation that authorizes the processing of your personal data,

as you have not received any information about the unsettled business relationship and would like to review the

You have requested the right to process your personal data.

On 13 August 2018, he again asked the Applicant by e-mail to send it

the authentic statement on which the Letter of Request containing the Requested Payment was based.

In this letter, the Applicant also rejected the Applicant's letter dated 10 August 2018

call to identify himself.

The Applicant contacted the Customer on 17 August 2018 by post, which does not require identification

With application. In that letter, he requested that his personal data be deleted, as he considered that a

As a result of the alleged breach of contract, he obtained it without informing him in advance, and

challenged the lawfulness of the data processing of the Applicant. However, in that letter it did not request

a copy of the documents supporting the claim or any other information about your personal data

management. Since the III.1. with regard to e-mail inquiries in accordance with

Applicant could not identify the Applicant, thus exercising the Applicant's right of access

did not consider his application to be from the Applicant and the Applicant is of August 2018

In his mail of 17, he no longer had the right to access or issue copies

application for the exercise of that right. Accordingly, the Applicant did not infringe Article 15 (1) of the GDPR.

and (3) when exercising the Applicant’s right of access by e-mail

in the absence of identification of the Applicant.

III.3. Applicant's request for deletion of personal data

III.3.1. By e-mail dated 13 August 2018, the Complainant requested an e-mail from the Applicant

deletion of the address or not to link it to the other personal data of the Applicant. The Complainant

complained that the Applicant had not immediately deleted his e-mail address, or even a reply message

sent in which he was informed that he had not provided his identification data and therefore to him

you cannot provide information.

The Applicant's e-mail address was known to the Applicant in connection with the complaint handling procedure, and

in the absence of identification of the data subject, it did not link it to a specific claim, and therefore the

Applicant's email address is not based on a screenshot of the receivables management record

has been recorded in the claims management register in the same way as the complaint management register

nor does it contain it.

It can therefore be concluded that the Applicant complied with the Applicant 's request that

do not associate your email address with any other personal information, as you have not recorded your email address

system level, so he could not delete it from his records.

The Applicant acted in accordance with Article 12 (4) of the GDPR when it was identified as such

did not consider The Applicant was informed of his contact details in a reply message sent to that e-mail

the consequences of failure to identify the e-mail address requested by the Applicant

deletion.

III.3.2. The Applicant has complied with the Applicant's request for cancellation and all personal data

has deleted the assignee 's receivables from its registration system because […] has repurchased

Claim against the Applicant assigned to the Applicant. The Requested 2018.

By letter dated 29 August 2006, the applicant further informed the applicant that his personal data were still available

can be found in the backups of the Applicant's IT system.

A Hpt. 67 / A. § (1) with the IT systems used by financial service providers

requirements for the IT system of financial institutions

Government Decree on the Protection of § explains in more detail, ie it determines how financial enterprises must comply with

the requirements prescribed in the Credit Institutions Act. One

such a criterion is that the data backup and recovery order of the live system is provided by the system

secure restore, and this requires backups of the system

be prepared. The IT system is a prerequisite for making backups and copies

the safe operation of the Receivables and the continuation of the Receivables Purchasing Activity,

as a result, with regard to the personal data contained in the backups, the

the legal basis for data processing is a legal obligation under Article 6 (1) (c) GDPR.

Despite the fact that Infotv. According to Section 5 (3), mandatory data processing is only required by law

may be prescribed by a municipal decree authorized by law, financial institutions

under the Government Decree on the Protection of the IT System

Data management is also considered mandatory data management, as Infotv. of the above provision a

the legislator is the addressee, not the law enforcers.

The Applicant as an enforcer is not in a legal position to be addressed to the legislature

assess the fulfillment of an obligation at a level of law which it considers inappropriate

in this regard, personal data

may also base its management on the provisions of a government decree as a norm requiring mandatory data processing.

As a law enforcement body, the Authority

nor may it be disregarded as long as that State is entitled to do so

body, in this case the Constitutional Court, in the appropriate proceedings, by the competent bodies or

unless otherwise provided by the parties.

In view of the above, the Applicant has complied with Article 17 (3) (b) of the GDPR

has not lawfully complied with the Applicant 's request that his / her personal data be processed by the Applicant a

also delete it from backups immediately.

III.3.3. The St. Pursuant to Section 169 (2), the accounting records are directly and indirectly
the supporting accounting document must be in a legible form for at least 8 years, the accounting records
retrievable in a retrievable manner. The accounting document is the Act. 166.
§ (1), for example, the invoice, the contract, the agreement, which is the economic event
supporting its accounting.
The contract concluded between […] and the Applicant and the contract in which
[…] repurchased its claim from the Applicant against the Applicant as an accounting document
shall be deemed to have been granted to the Applicant in accordance with the provisions of Art. it must be kept for eight years.
THE
The legal basis for the processing of personal data contained in accounting documents is Article 6 (1) of the GDPR.
Article 17 (3) (b) of the GDPR cannot be deleted at the request of the Applicant either.
in accordance with
III.3.4. A Hpt. Section 288 (3) provides that the financial institution shall file a complaint and file a complaint
retains a given answer for five years. This is supplemented by Section 3 (2) of the Government Decree on Complaints
by informing the financial institution about customer complaints and their resolution,
keep a record of the measures taken to resolve it. The complaint handling register
it must include, inter alia, a description of the complaint, the event or fact which is the subject of the complaint
marking.
Consequently, the Applicant's legal obligation under Article 6 (1) (c) of the GDPR
lawfully manages the name of the Applicant and the Applicant in the complaint handling register
data on the complaints submitted by the Hpt
Nor may it be canceled at the request of the applicant.
Acting lawfully in accordance with the provisions of this GDPR, the
Applicant, when only partially, complied with its claim management records a
Request for deletion of the applicant's personal data.

III.4. The requirement of transparency

Transparency must be present throughout the data management process, ie not only that

concerned GDPR 13-14. but for the exercise of the rights of the data subject

when examining and responding to requests.

The Applicant in its reply to the Applicant's request for cancellation dated 29 August 2018

informed the Applicant that he would also delete his personal data from the backups, but only then

and if this is a backup during a restore, the backups

in accordance with its rules. If the particular backup - the backup

shall be deleted in its entirety in accordance with its rules on copies

data.

The “Backup and restore operational

procedure ”is not public, neither for the data subjects, nor for the Applicant

available. As a result, the Applicant did not properly inform the Applicant that

which is the last backup that still contains your personal information, what

In some cases, backups may be used, or when not

the Applicant deletes the last backup that was included before the deletion

personal data of the Applicant. In view of the above, the Applicant has violated Article 5 (1) of the GDPR.

the principle of transparency referred to in paragraph 1 (a).

III. 5. Legal Consequences

III.5.1. The Authority grants the Applicant's request in part and Article 58 (2) (b) GDPR

condemns the Applicant for violating Article 5 (1) (a) of the GDPR

and Article 12 (2) and Article 58 (2) (c) of the GDPR

instructs the Applicant to inform the Applicant containing his personal data

the date when the backups were deleted and the use of the backups

conditions.

III.5.2. The Authority rejected the Applicant's imposition of the fine or the Authority's decision

- Infotv. Pursuant to Section 61 (2) of the Public Procurement Act, as e

the application of legal consequences does not directly affect the right or legitimate interest of the Applicant,

such a decision of the Authority shall not create any right or obligation for it

With regard to the application of legal consequences in the public interest,

the imposition of fines and the publication of the decision with identifying data by the Applicant

does not qualify as a customer under Ákr. § (1) of the Act, or - as the Act no. Section 35 (1)

does not comply with paragraph 1, there is no need to submit an application in this regard, the submission

this part cannot be construed as an application.

III.5.3. However, the Authority examined of its own motion whether it was justified in respect of the applicant

imposition of a data protection fine. In this context, the Authority will amend Article 83 (2) of the GDPR and Infotv.

75 / A. § considered all the circumstances of the case.

First of all, the Authority took into account that the violations committed by the Applicant are the result of the GDPR

They constitute a more serious infringement within the meaning of Article 83 (5) (a) and (b). In addition, the

the breach found is attributable to the Debtor, the Debtor is liable for the exercise of the right in question

subject to the provisions of the GDPR, subject to the above

in accordance with the provisions of the GDPR, effectively hindering it.

In imposing the fine, the Authority also took into account that the Requested Offender

his conduct in the particular case may in fact have contributed to the exercise of the rights of the person concerned being lower

and the infringements found may also have contributed to the Applicant’s

only belatedly and the wider rights originally planned - and due to him

he could not practice. It is therefore necessary to impose a fine on the Applicant specifically,

or, in the case of similar data controllers, in general, in order to prevent further infringements

despite the fact that in the present case there is an infringement relating to the exercise of the rights of a single data subject

weave..

In view of the above, as well as the fact that the Debtor according to its 2017 financial statements is subject to the current year

its pre-tax profit was nearly HUF 20 billion, the data protection fine imposed is a symbolic

and does not exceed the maximum fine that may be imposed.

The amount of the fine was determined by the Authority acting in accordance with its statutory discretion.

Based on the above, the Authority has decided in accordance with the operative part.

ARC. Other issues:

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

covers the whole territory.

15

The decision is based on Ákr. 80.-81. § and Infotv. It is based on Section 61 (1). The decision is based on Ákr. § 82

Shall become final upon its communication pursuant to paragraph 1.

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) by decision of the Authority

The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (11)

the Metropolitan Court has exclusive jurisdiction. 2016 on Civil Procedure

CXXX. Act (hereinafter: Pp.) - the Kp. Applicable pursuant to Section 26 (1) - Section 72 provides for legal representation in a case falling within the jurisdiction of the Tribunal. Kp. Section 39 (6)

unless otherwise provided by law, the date of filing of the application

has no suspensory effect on the entry into force of an 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 referred to as the Customer's legal representative pursuant to Section 9 (1) (b) of the E-Administration Act

obliged to communicate electronically.

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

Information on the possibility of requesting the maintenance of the It is based on § 77 (1) - (2). THE

the amount of the fee for an administrative lawsuit in accordance with Act XCIII of 1990 on Fees. Act (hereinafter:

Itv.) 44 / A. § (1). From the advance payment of the fee, the Itv. Section 59 (1)

and Section 62 (1) (h) shall release the party initiating the proceedings.

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

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

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

decision of the Ákr. Pursuant to Section 82 (1), it becomes final with the communication. The Ákr. Section 133

enforcement, unless otherwise provided by law or government decree

ordering authority. The Ákr. Section 134 of the Enforcement - if law, government decree

or in the case of a municipal authority, a decree of a local government does not provide otherwise

carried out by a state tax authority. Infotv. Pursuant to Section 60 (7) in the decision of the Authority

to perform a specific act, conduct or tolerate a specific act

the Authority shall enforce the decision in respect of the standstill obligation

implements.

Budapest, February 20, 2019

Dr. Attila Péterfalvi

President

c. professor