Case number: NAIH / 2019/167/13.

History case number: NAIH / 2018/7142 / 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”), the […] (hereinafter referred to as the “Applicant 1”) and the […]

hereinafter referred to as the Applicant 2) (hereinafter together referred to as the Applicants)

take the following decisions in the data protection authority procedure:

I. The Authority will convict the Applicant of unlawful data processing and

request for the deletion of your personal data

as follows:

I.1. It states that the Applicant 1 in connection with the personal data of the Applicant

violated the Applicant’s right of access and is transparent and fair

the principles of data management, accuracy and accountability.

I.2. It finds that Applicant 2 is being treated by the Applicant on the basis of an inappropriate legal basis

personal data and in connection with the processing of the Applicant's personal data

violated the principle of accountability.

II.1. It ex officio obliges Applicant 1 to initiate a judicial review

the expiry of the relevant time limit for bringing an action or, in the case of a review, the court

within 15 days of the decision of the applicant to the Applicant and the Authority if there is a legitimate interest in

Applicant's personal data and this interest in the Applicant's fundamental rights

and inform the Applicant of his right to protest,

and how to practice it!

II.2. It ex officio obliges Applicant 2 to initiate a judicial review

the expiry of the relevant time limit for bringing an action or, in the case of a review, the court

within 15 days of the decision of the applicant to the Applicant and the Authority if there is a legitimate interest in

Applicant's personal data and this interest in the Applicant's fundamental rights

and inform the Applicant of his right to protest,

and how to practice it!

II.3. It obliges the Applicants ex officio that until they comply with the conditions set out in II.1. and II.2. point

in the meantime, restrict the processing of the Applicant's personal data.

II.4. It ex officio obliges Applicant 1 to initiate a judicial review

the expiry of the relevant time limit for bringing an action or, in the case of a review, the court

send the contracts to the Applicant's legal representative within 15 days of the decision

a copy of the audio recordings of the conference calls - on the audio recording

without prejudice to the rights of other persons included in the contract - and provide information to the Applicant

about the personal data processed about it in the customer registration system!

III.1. Due to illegal data processing, I requested 1 ex officio

HUF 2,000,000, ie HUF 2 million

data protection fine

2

obliges to pay.

III.2. Due to illegal data processing, he requested 2 ex officio

HUF 1,000,000, ie one million forints

data protection fine

obliges to pay.

ARC. The part of the request for the Authority to order the deletion of personal data shall be:

Authority rejects.

V. The part of the application aimed at banning the Applicants from the Applicant's personal data

the Authority shall reject it.

The expiry of the time limit for bringing an action for judicial review,

or, if a review is initiated, within 15 days of the decision of the court

centralized revenue collection target settlement forint account (10032000-01040425-00000000

Centralized direct debit IBAN: HU83 1003 2000 0104 0425 0000 0000)

to pay. When transferring the amount, NAIH / 2019/167 / H. JUDGE. number should be referred to.

If the Debtors fail to meet their obligation to pay the fine on time, it shall be delayed

they are required to pay a supplement. The rate of the late payment interest is the statutory interest, which is in arrears

equal to the central bank base rate valid on the first day of the calendar half-year concerned.

A II. 1. and II. Obligations under point 2 and fines and penalties for late payment shall not apply

the Authority shall order the enforcement of the decision.

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.

The Authority draws the attention of the Applicants to the fact that it is open to challenge the decision

until the expiry of the time limit for bringing an action or, in the case of an administrative lawsuit, until a final decision of the

court a

data affected by disputed data management cannot be deleted or destroyed!

EXPLANATORY STATEMENT

(1)

I. Procedure and clarification of the facts

(2)

I.1.1. Authorized legal representative of the Applicant to the Authority November 2018

In its request received on the 30th day, it initiated the initiation of data protection official proceedings.

(3)

In his application, the Applicant stated that he wanted to conclude a subscription contract in April 2018

Applicant 1, however, Applicant 1 refused to enter into a contract for it

with reference to the records of the Applicant's previous service

outstanding debt arising from contracts, which arose in June 2017

Assigned to 2 assigned. The Applicant contacted both Applicant 1 and Applicant 2 regarding the debts as they had not

previously been contracted.

in a legal relationship with Applicant 1, and therefore could not even owe any debt to him.

3

(4)

By letter dated 5 June 2018, the Applicant requested information from 1 that

whether the personal data contained in the form attached to it is the same as that of the debtor

with the data against whom your claim is Claimant 1 Claimant 2

conceded. He also requested information on whether Applicant 1 had any

a document certifying that the debtor of the assigned claims

personal data is the same as the Applicant's personal data and such

if a document exists, requested a copy of that document.

(5)

Applicant 1 In its reply dated 2 July 2018, claiming that the contract

the purpose of the processing is the termination of the legal relationship and the assignment of the claim

has ceased to exist and the data relating to the subscriptions have been deleted from its register,

did not provide information on the handling of the Applicant's personal data. This response was issued in 2018.

confirmed in a letter dated 25 October.

(6)

By letter dated 15 October 2018, the Applicant requested information from Applicant 2 that

on the basis of which documents, which manages your personal data, however, Applicant 2.

refused to reply, the power of attorney given by the Applicant to his representative

reference to its shortcomings.

(7)

When the Applicant first contacted the Applicant 2

customer service, you did not receive information about the processing of your personal data there because

the name of the mother provided for identification did not match in the records of Applicant 2

with the actor. This data was subsequently provided by the Applicant

on the basis of a copy of his identity card Requested by 2.

Applicant 2 further informed the Applicant that the […], […],

[…] In order to enforce claims registered under number already had judicial enforcement

is in progress.

(8)

In view of the above, the Applicant requested that the Authority condemn the Applicants to a

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

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

infringement of the provisions of Regulation (EU) No 2016/679 (hereinafter referred to as the GDPR),

prohibit Applicants from further processing of their personal data and oblige the

Requested to delete your personal information. At the request of the Applicant, the information

CXII of 2011 on the right to self-determination and freedom of information Act (a

hereinafter: Infotv.) pursuant to Section 60 (1) of the NAIH / 2018/7142 / H. case number

data protection authority proceedings have been initiated.

(9)

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

to clarify the facts.

(10) Applicant 1 stated that it is a customer manager and registrar, as well as billing

in the system of […]; […]; […]; […]; […] Customer numbers or the name of the Applicant

data are not included for the year 1, as the contract with the subscriber has expired since 1

years + 30 days have already elapsed, as notified to the Applicant. To support this

attached screenshots of your records.

(11) According to the first statement of the applicant 1, it did not have any of the above customer numbers

contracts, only confirmation of the transfer of the contracts to the Authority

sent documents containing the [Applicant's name] and subscription

No additional personal information was included outside the location.

(12) There are five different names of the Applicant in different parts of the country

The contract of use […] was rewritten between 15 August and 26 September 2016.

between. Applicant 1 attached to his second statement the sound recordings on which

it is audible that subscriptions are initiated by a man who calls himself [the Applicant]

[…] Transcription in the name of a conference call in which the previous subscribers

also participated.

(13) According to the statement of the applicant 1, in the framework of a conference call by telephone

during contract rewriting, the transferring party is identified by a customer number, while the transferee

in the case of a party, in order to establish his identity

personally identifiable information is required. During the conference call, the [a

As the place and date of birth of the man introducing himself as the Applicant], the Applicant 's place of birth

and the number of the Applicant's identity card […],

however, to her mother’s name question, she only answered once that [the Applicant’s mother

name], the other times entered […].

(14) Applicant 1 in its reply of 29 January 2019 to the Authority's question on what

records and on what basis the employee refused to contact the Applicant

on 24 April 2018, referred to the 2003 Act on Electronic Communications

C. (hereinafter: Eht.), However, did not provide an answer,

whether it handles the Applicant's personal data with reference to this law.

Requested 1 only by the Authority NAIH / 2019/167/6. repeated in his order no

upon request, provided information that the Applicant 1 has a unified customer register

there is a system that has different levels of access and different access rights. THE

In order to prevent fraud, subscribers who have a new contract

risky, special marking. Certain personal information of these subscribers is

are kept in a part of the customer record system for which they are special

access permission is required. Record this section with the Applicant

deals with the place and time of birth and four different ones

mother's name data: […], […], […], […]. Requested 1 was spoken on the audio recordings

nevertheless attributes to the Applicant on the basis of the identity card number

all debts under the name of [Applicant] that his mother's name is given for the four debts

significantly different. Management of this data for fraud prevention purposes

as the legal basis of the Applicant 1 in the statement of the Eht. Received in Section 158 (1)

has a legitimate economic interest. As the Applicant

The amount of debt attributed to him was HUF 623,854, so Claim 1 according to the frauds

legitimate interest in the prevention of

by restricting the right to privacy.

(15) According to the statement of Applicant 1, the Applicant did not provide a substantive answer in June 2018

Request to exercise his right of access dated 5

submitted it through a channel dedicated to the exercise of the rights of the data subject, and was therefore unable to do so

necessary measures.

(16) I.1.3. According to the Applicant's 2 statements, the Applicant's personal data will be processed in accordance with Article

6 (1) of the GDPR.

paragraph (b), the performance of the contract shall be governed by a legal basis. The contract for which

In its opinion, the processing of the Applicant 's personal data is necessary for the fulfillment of the

assignor, ie the subscription contract between Applicant 1 and the Applicant. The

a claim arising from the non-payment of a fee arising from a subscription contract

was the subject of an assignment agreement between Applicant 1 and Applicant 2,

Thus, Applicant 2 considers that the fulfillment of this scope is subject to personal data

and to enforce claims against the Applicant. Requested 1 a

upon the transfer of the claim, it was made available to the Claimant 2 by the basic contract

personal data included in the assignment agreement

in the data table, however, Requested 2 with the subscription contract itself or its

does not have a copy.

5

(17) As set out in Annexes 9 and 19 to the Applicant's reply of 31 January 2019

The 2 employees of the Applicant requested data reconciliation regarding the Applicant

referring to “only an electronic contract is available in which it is personal

data are not indicated ”and“ no document has been transmitted on which

the data would be included. " Applicant 2 was also unable to present the request at the request of the Authority

Applicant and Applicant 1 have entered into contracts for which data management

he founded. Applicant 2 takes the view that the claims are assignment and not

acquired by contract, therefore more information about the contract

not necessary for its possession.

(18) The number of the Applicant's identity card was indicated on the data plate, so he knew

Applicant 2 a copy of the identity card submitted by the Applicant

also include claims for which the mother's name is data

did not match the Applicant's mother's name.

(19) I.1.4. The Authority contacted the Ministry of the Interior, which is responsible for keeping records

Deputy State Secretariat Personnel Registration and Administration Department Domestic

Department of Legal Aid and was informed that personal data - and

the place of birth of the person named [Applicant] is not in the address register: […],

date of birth: […], mother's name: […] with details.

(20) II. Applicable legal provisions

Pursuant to Article 2 (1) of the GDPR, the processing of data in the present case requires the GDPR apply.

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

Recital 39: The processing of personal data is lawful and it must be fair. It must be transparent to natural persons that: how they collect and use their personal data about them considered or otherwise treated, and in the context of a the extent to which personal data is or will be processed. The principle of transparency requires that information relating to the processing of personal data, or communication is easily accessible and comprehensible and that it is clear and they are worded in simple language. This principle applies in particular to those concerned with the identity of the controller and the purpose of the processing further information to ensure the fairness of the personal data of the data subject and transparent management, as well as the information that data subjects have a right receive confirmation and information about the data processed about them. The natural person a the risks, rules, guarantees and implications of the processing of personal data rights and how to exercise it in relation to data processing rights. Above all, the specific purposes of personal data processing are explicit and lawful, as well as the collection of personal data must be specified at the time of Personal data for the purpose of their processing they must be appropriate and relevant and the range of data required for the purpose should be kept to a minimum. To do this, you need to ensure in particular that you are personal data storage should be limited to the shortest possible period of time. Personal information only they may be handled if the purpose of the data processing is otherwise reasonable it is not possible to achieve. To ensure that the storage of personal information a

limited to the time required, the controller shall delete or periodically review it

sets deadlines. To correct or delete inaccurate personal information

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

6

ensuring an adequate level of security and confidentiality, including

in order to prevent personal data and personal information

unauthorized access to or use of the devices used to deal with them

use.

GDPR Recital 44: Data processing is lawful if it is

required under a contract or intention to enter into a contract.

GDPR Recital 63: The data subject has a right of access to the data subject

to the data collected and that, at simple and reasonable intervals, the

exercise this right in order to establish and verify the lawfulness of data processing.

(…)

GDPR Article 5 (1) (a) to (c) and (2): 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 accurate and, where necessary, kept up to date; all reasonable measures

should be done in order to be inaccurate for the purposes of data processing

personal data must be deleted or rectified without delay ("accuracy").

2. The controller shall be responsible for complying with paragraph 1 and shall be able to

to demonstrate this compliance (‘accountability’).

GDPR Article 6 (1) (b) and (f): Processing of personal data only if and

is lawful if at least one of the following is met:

(b) processing is necessary for the performance of a contract to which the data subject is party

at the request of the party concerned or before the conclusion of the contract

necessary to do so;

(f) processing for the legitimate interests of the controller or of a third party

necessary, unless those interests take precedence over such interests

interests or fundamental rights and freedoms that protect personal data

especially if the child concerned.

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 of the fact that the

the person concerned may lodge a complaint with a supervisory authority and have recourse to the courts

with the right.

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

receive information on whether your personal data is being processed and if

such data processing is in progress, the right to access personal data and

access to the following information:

(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, failing that

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 limitation of the handling of such personal data

against data processing;

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

(g) if the data were not collected from the data subject, all available sources

information;

(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

comprehensible information on the significance of such data processing and the

the expected consequences for the data subject.

Article 15 (3) GDPR: The controller is the personal data subject

provide a copy of the data to the data subject. Additional requested by the data subject

for copies, the controller shall charge a reasonable fee based on administrative costs

you can charge. If the person concerned submitted the application electronically, the information shall be extensive

shall be made available in an electronic format widely used, unless

concerned requests otherwise.

Article 58 (2) (b), (c), (g) and (i) GDPR: The supervisory authority shall take corrective action

acting under the authority of:

(b) reprimands the controller or the processor if he or she is acting in a data-processing capacity

has infringed the provisions of this Regulation;

(c) instruct the controller or processor to comply with this Regulation

the exercise of his rights under this Regulation;

(g) order personal data in accordance with Articles 16, 17 and 18 respectively

rectification or erasure of data and restrictions on data processing, as well as Article 17 (2)

order notification to the addressees in accordance with

with whom or with whom the personal data have been communicated;

(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

ensure that any infringement of this Regulation referred to in paragraphs 4, 5 and 6 is in accordance with this Article

The administrative fines imposed pursuant to this Regulation shall be effective, proportionate and dissuasive in each case

be dissuasive.

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

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

In deciding whether it is necessary to impose an administrative fine, or a

the amount of the administrative fine in each case

the following must be taken into account:

(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 the infringement; and

the extent of the damage they have suffered;

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

(c) the damage suffered by the data subject by the controller or the processor

any measures taken to alleviate

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

the technical and organizational measures taken pursuant to Articles 25 and 32;

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

(f) with the supervisory authority, remedy the breach and the breach may be negative

the degree of cooperation to mitigate its effects;

(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

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

in detail;

(i) if previously against the controller or processor concerned, in the same

have ordered one of the measures referred to in Article 58 (2),

compliance with the measures in question;

(j) whether the controller or processor has complied with Article 40

approved codes of conduct or an approved certification in accordance with Article 42

mechanisms; and

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

for example, the financial gain obtained as a direct or indirect consequence of the infringement

or avoided loss.

5. Infringements of the following provisions, in accordance with paragraph 2, shall be imposed no later than 20

An administrative fine of EUR 000 000 or, in the case of undertakings, the previous

an amount not exceeding 4% of its total annual worldwide turnover for the financial year,

with the higher of the two:

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

appropriately;

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

In order to enforce this, the Authority may initiate ex officio data protection proceedings. The

CL of the General Administrative Procedure Act 2016 on the data protection authority procedure.

(hereinafter: Ákr.) shall be applied in accordance with the provisions of the Infotv

additions and derogations under the General Data Protection Regulation.

Infotv. Pursuant to Section 61 (6), an action may be brought to challenge a decision

until the expiry of the term or, in the case of the commencement of an administrative decision, until the final decision of the

court a

data affected by the disputed data processing may not be deleted or destroyed.

Infotv. 75 / A. § according to Article 83 (2) - (6) of the General Data Protection Regulation

exercise the powers set out in paragraph 1 in accordance with the principle of proportionality,

in particular by providing for the law or regulation on the processing of personal data

Requirements laid down in a binding act of the European Union

to remedy the breach - Article 58 of the General Data Protection Regulation.

in particular by alerting the controller or processor

to take action.

Section 158 (1) of Act C of 2003 on Electronic Communications: Electronic

telecommunications service providers for the payment of fees and other obligations arising from the contract

prevention of circumvention and the conditions specified in Section 118 (4)

if they exist, they are entitled to refuse to enter into a contract pursuant to Section 157

the data necessary to identify the subscriber from the range of legally manageable data,

and information on the reason for the transfer pursuant to paragraph 3

to or from an electronic communications service provider

create a common dataset.

(21) III. Decision

(22) In the present proceedings, the Authority is only the request for the requested processing

examined the data processing at the time of submission and the subsequent period

accordingly, although the history of data management is earlier, before 25 May 2018

did not make any findings regarding the data processing carried out by the

(23) III.1. Data management of 1 requested

(24) III.1.1. Principle of accountability

(25) Applicant 1 stated that the personal data of the Applicant were processed by Eht. Section 158 (1)

in accordance with its legitimate economic interest

for fraud prevention purposes.

(26) The Eht. Section 158 (1) authorizes electronic communications service providers to

that the subscriber is evading a fee or other contractual obligation

in order to prevent or Conditions specified in Section 118 (4)

to identify subscribers for the purpose of refusing to conclude a contract

the necessary personal data are transferred or taken over by other service providers, or

transmitted to the common database.

(27) Applicant 1 stated that Eht. The data management contained in Section 158 (1)

none of the operations took place, no common dataset was created, however

both the transfer of data and the receipt of data is a prerequisite for the transfer of data to electronic communications

stored in its own records. For this reason, the Eht. 158. (1)

for the purposes of electronic communications providers

Applicant 1 may be entitled to his / her personal data based on his / her legitimate interests

to be stored in a customer register system and to be specially marked.

(28) However, Applicant 1 did not demonstrate to the Authority that it had a legitimate interest

appropriate balance of interests in support of its interests, did not specify what

fraud or repeated attempts to prevent fraud, which is personal

how data management serves and the extent to which that data is necessary and appropriate

to achieve the goal of fraud prevention. Requested 1 did not compare by their own data management

with the rights and interests of the Applicant, not the weighting between them

priority of his own interests over the rights and interests of the Applicant

confirmed. It is in itself that the Applicant may owe or the Applicant 1

attributes a debt to it does not legitimize the data processing it carries out. Especially not

the Applicant 1 has confirmed that the data processing of the Applicant is specific to the

the personal data of the Applicant is actually necessary and possible for the purpose indicated

proportionate to its interests and to its fundamental rights and freedoms.

(29) Based on the principle of accountability to data controllers throughout the data processing process

they must implement data management operations in such a way as to be able to protect their data

to demonstrate compliance with the rules. The principle of accountability, so not only

in general, can be interpreted at the process level, all specific data management activities,

also applies to the processing of the personal data of a specific data subject.

(30) The controller is responsible for the lawfulness of the data processing carried out by him. Article 6 (1) of the GDPR

Due to the nature of the legal basis under paragraph 1 (f), the controller who

plea relies must be able to accurately indicate that a specific personal data

which legitimate interest of the controller is justified and why

it is necessary to manage the data, at the same time to prove and prove it to have priority

enjoy the legitimate interests, fundamental rights and freedoms of the data subject.

(31) Legal basis indicated as the legal basis for data processing and data processing on that basis

in the absence of a need for and a justifiable balance of interests with the data subject

Applicant 1 did not qualify for accountability under Article 5 (2) GDPR

principle.

10

(32) III.1.2. Ensuring the exercise of the Applicant 's right of access and transparent and

principle of fair data management

(33) Acting on behalf of the Applicant […] lawyer Applicant 1 [in the Privacy Policy]

sent by the Applicant as a registered post to the address indicated as the contact address […]

including a request for the exercise of the right of access and the right to issue a copy,

Letter dated 5 June 2018, certified by a copy of the consignment note.

(34) Consequently, the claim of Applicant 1 that it was unable to

request the necessary measures because of the exercise of the right of access

the Applicant is not through an official channel dedicated to the exercise of the rights of the data subject

submitted by the data subject of the Data Protection Policy of the Applicant 1

Applications must be submitted by post to the above address and there is no other alternative post office

availability. However, in the Authority's view, Applicant 1

must also accept and comply with the data subject's requests if the data subject does not

submit it through a designated channel, as requests for the exercise of the rights of the data subject

shall not be limited to a single channel of communication. Requested 1

nor is this claim admissible because Applicant 1 at the request of the Applicant above

He replied on July 2, 2018, judging it.

(35) The Applicant for the exercise of the right of access to Applicant 1 dated 5 June 2018

Applicant 1 informed that the contractual relationship

information cannot be provided because of the contractual relationship

by the termination of the claims and the assignment of the claims to the Debtor 2

The purpose of data management has been terminated, therefore the data related to the subscription has been deleted a

from the register.

(36) The above information provided by the applicant 1 did not correspond to reality, as dated 28 February 2019

according to his statement, they were still found at one level of the customer record system

the Applicant's personal details and also provides for those conference calls

with the sound recordings of which its subscribers were transcribed to [Applicant's name]

contracts.

(37) The Authority emphasizes that if the data subject wishes to exercise his right of access,

so, also in view of the content of the application, it is not sufficient to be included in certain registers

provide information on the data. The information must be provided for all personal data

which is held by the controller in relation to the data subject, regardless of whether the

where and in what form the data is available - complaint register,

backup, paper or electronic accounting document, correspondence and related

what data management operations you perform (such as storage, archiving, etc.).

(38) Applicant 1 has the task and responsibility to assess in which records, what

personal data and, if requested by the data subject, shall be subject to the provisions of Article 15 of the GDPR.

provide access in accordance with Article

(39) The applicant 's request for access rights was not limited to 1

customer registration system or that part of it for which it is not required

special access right. It was clear from the application that access

The reason for filing the application for the exercise of the right was that the Applicant 1 refused to

concluding a contract with the Applicant referring to previous debts. For this reason, He requested

1 should have recognized the need to involve one of his co-workers as well

in the assessment and fulfillment of the access request, who has the customer record

with special, wider access rights to the system.

11

(40) The applicant also requested information on whether Applicant 1 had any documents

to substantiate that the assigned claims are fixed by the debtors

personal data is the same as or requested by the Applicant

copies of documents. The Applicant is not expected to be aware of the Applicant

1 with the processes of concluding contracts and rewriting contracts, therefore the contracts are based on this application

and as one of the participants in the Applicant 1

audio recordings of the recorded conference calls were also available to the Applicant

would have forgiven Applicant 1.

(41) Applicant 1 informed both the Applicant and the Authority that if

Applicant notices that his personal data has been misused and is therefore police

make a report, which is confirmed by the customer service of the Applicant 1, so

Claimant 1 repurchases the claims from Claimant 2 and is uncollectible

as receivables, the Applicant does not have to pay them. Requested 1 no

facilitated the Applicant 's use of this possibility, as it was untrue and

misleadingly informed that he does not handle his personal data, and thus the Applicant

he was not able to access that information — especially about those conference calls

for sound recordings on which the contracts have been transcribed in his name - which

could have learned on the basis of how the Applicant 1 became the property of the

personal information. In the absence of this information, he could not be convinced that it was being abused

happened to your personal information. It also prevented Petitioner from being

any right relating to the processing of personal data, in particular in this case Article 21 of the GDPR

the right to protest under

(42) Applicant 1 by providing false information to the Applicant about his personal data

which resulted in the Applicant not providing any information on the merits

did not receive data processing or be granted access to the contracts

infringed Article 15 (1) and (3) of the GDPR.

(43) Transparency should apply throughout the data processing process. Transparency

principle, it should be transparent to data subjects which personal data,

which data controllers, how they are handled. One way to make sure of this is the right of access

in which data subjects can verify the lawfulness of data processing.

(44) By requesting 1 of Annex III.1.2. untrue and misleading as set out in

provided the Applicant with information on the processing of his personal data, according to which he deleted

so you can’t provide more information about it and contact Debtor 2 - impossible

made it possible for him to see through the processing of his personal data by the Applicant 1,

in breach of Article 5 (1) (a) of the GDPR, which is transparent and fair

principle of data management.

(45) III.1.3. Accuracy requirement

(46) Applicant 1 has the Applicant's name, date of birth and four different mother's name details

manages in its records.

(47) According to the statement of Applicant 1, the amount of debts attributed to the Applicant is 623 854

HUF - six hundred and twenty-three thousand five hundred and sixty-four forints - which is only possible if

Applicant 1 for all five […] [Applicant Name]

It is considered to be an applicant, regardless of whether it is exclusively for the transfer of contract […]

The man who called himself [Applicant's name]

that her mother 's name is [Applicant' s mother 's name], while the other recordings say that

mother's name is […] or […]. So the personal data provided by the recipient of the contract

12

only in respect of contract No […] are the same as in

With the personal data of the applicant.

(48) The register of personal data and address does not contain a person whose name

and the place and date of birth are the same as those of the Applicant and the name of the mother is […] or […].

(49) In the context of one of the debts, the name […] appears in the register as the name of the mother

data, but this was not reflected in any of the conference talks on the rewriting of the contract

so the accuracy of this data is also in doubt.

(50) Regarding the accuracy of personal data, more than 1 requested data processing

could have been in doubt, for example on 10 May 2018, when

contacted Applicant 1 to investigate the complaint submitted to him by the Applicant

and when contacted by the Applicant by letter dated 5 June 2018

He applied for 1, inter alia, to exercise his right of access.

(51) Irrespective of when the personal data of the Applicant were in doubt

in relation to the accuracy of, is in itself that Applicant 1 with the same person, a

In connection with the applicant, the names of four different mothers handle data in breach of Article 5 of the GDPR

The accuracy requirement of paragraph 1 (d).

(52) III.2. Requested 2 data management

(53) III.2.1. Legal basis for the requested 2 data processing

(54) III.2.1.1. According to the statement of the Applicant 2, the legal basis of its data processing is the Applicant 1 and the

Performance of contracts between the applicant, as they gave rise to claims

acquired by Applicant 1 by assignment.

(55) The Authority finds that the legal basis under Article 6 (1) (b) of the GDPR, namely the

with the exception of certain pre-contractual steps, is only applicable if a

necessary for the performance of the contract, so that this plea cannot be extended to

data processing operations for which the situation is due to the non-performance of the contract by the data subject

steps resulting from the normal duty of cooperation of the Contracting Parties

required to do so. The performance of the contract may also include steps

when the controller who concluded the contract with the data subject - that is, who in the contract a

the other party - in the event of a delay in performance, calls on the person concerned to perform. However, the GDPR

The contractual basis referred to in Article 6 (1) (b) shall no longer apply to

in the event that the controller has a claim against the data subject for non-performance

to a debt collection company (ie the problem has already been

out of contract). Data transfer in the context of assignment

its legal basis is thus limited to the claimant's own claim, typically on the part of the assignee

may have a legitimate interest in enforcing it.

(56) According to the reasoning attached to the Civil Code, the transfer of claims by transfer of ownership

is based on the same logic, so the assignment is in fact nothing more than

transfer of ownership of a claim.

(57) The assignment separates the claim from the original legal relationship from which it arises, and

the assignee enters only in respect of the claim and not in respect of the fundamental relationship

in place of the assignor. By assigning the claim to the

from the fundamental right and the assignee becomes the holder of the claim, the claim

the concessionaire's enforcement and the related data management are no longer valid

in order to perform the contract from which the claim originally arose,

whereas in this case the assignor is not for his own benefit but for the benefit of the assignor

the claim acquired by assignment should be enforced. The

by assignment, if for consideration, to the assignor

will be fully or partially recovered depending on the purchase price. The

the concessionaire acts in his own interest and for his own benefit in order to recover the claim, since

by assignment, he becomes the holder of the claim, and the enforcement of the claim, the debtor

enforcement and the processing of data for that purpose is in his legitimate interest, no

and serves to fulfill the underlying contract, as the claim is by assignment

became independent of the contract.

(58) As Applicant 2 acquired through assignment attributed to the Applicant

claims and, as a consequence, the personal data of the Applicant, and thus the

claims, the legal basis for its processing cannot be Article 6 (1) of the GDPR.

contractual legal basis under paragraph 1 (b).

(59) In view of the above, Applicant 2 infringed Article 6 (1) of the GDPR by failing to do so

processed the Applicant's personal data with reference to an appropriate legal basis. However, this is not the case

necessarily means that there is no legal basis for the processing of the Applicant's personal data

none, as the lawful purchase of receivables permitted by law

obtained the Applicant's personal data in the framework of his / her activities - natural

personal data and the details of the claim - and lawfully

to enforce the acquired claims and the above data required for this purpose

there was a legitimate interest in treatment as a result of the legislation.

(60) III.2.1.2. Applicant 1 in both the letter to the Applicant dated 2 July 2018 and the

In its first reply to the Authority's request, it stated that the contracts

from which the claims assigned to Claimant 2 arose ceased to exist, i

There is no valid and valid contract between Applicant 1 and the Applicant.

(61) This fact is further confirmed by the letter dated 29 May 2018 from the Applicant 2 to the Applicant.

letter in which Applicant 2 provides information that Applicant 1 is not

between the Applicant 1 and the Applicant with respect to the performance

contracts and then assigned its material claims after the termination of the contract

He applied for 2.

(62) A precondition for the processing of data under Article 6 (1) (b) of the GDPR, if

not to take action at the request of the data subject prior to the conclusion of the contract

to exist and for the contract to be valid and valid

the data is processed with reference to its fulfillment.

(63) Applicant 2 therefore performed the performance of contracts with reference to the performance of personal data

contracts which have been terminated, ie are not capable of producing legal effects. From this

Due to this, Applicant 2 could not have lawfully invoked his data processing even then

Article 6 (1) (b) of the GDPR, if it were otherwise

the appropriate legal basis for the processing of personal data.

(64) III.2.2. Principle of accountability

(65) Based on the principle of accountability to data controllers throughout the data processing process

they must implement data management operations in such a way as to be able to protect their data

to demonstrate compliance with the rules. So the principle of accountability is not just that

in general, can be interpreted at the process level, all specific data management activities,

also applies to the processing of the personal data of a specific data subject.

(66) The controller is responsible for the lawfulness of his data processing, not this responsibility

can be transferred to another. Contractual legal basis under Article 6 (1) (b) GDPR

due to the nature of the personal data to the controller who invokes this legal basis

must be able to prove that the contract which

handles personal data with reference to its performance, existing, valid and valid, not here

including taking steps at the request of the data subject prior to the conclusion of the contract. This

regardless of whether it is a civil law or other matter specific to the legal relationship

whether you should have a contract under the rules.

(67) Therefore, as Applicant 2 could not demonstrate the existence of

The contract concluded between the Applicant and the Applicant 1, to which the

Personal data of the applicant and nevertheless in accordance with Article 6 (1) (b)

therefore did not comply with Article 5 (2) of the GDPR

the principle of accountability.

(68) III. 3. Legal Consequences

(69) III.3.1. The Authority grants the Applicant's request and Article 58 (2) (b) GDPR

condemns Applicant 1 for violating Article 5 § 1 of the GDPR

(a) and (d), Article 5 (2) of the GDPR and Article 15 (1) and (3) of the GDPR.

ex officio in accordance with Article 58 (2) (g) of the GDPR

orders the restriction of the processing of the Applicant's personal data until Applicant 1

certify that the legitimate interest in data processing takes precedence over the rights of the Applicant and

as he did not prove to the Authority in the course of the proceedings that he had those interests

actually performed the balancing between.

(70) Pursuant to Article 58 (2) (c) GDPR, the Authority will instruct Applicant 1 ex officio to comply with the Applicant's request

for access by sending the Applicant's legal notice.

representative

for

the

Applicant

personal

as data

registered

audio recordings of conference calls, and provide information on

personal data processed in the customer registration system. Position of the Authority

According to the Applicant, it is in his best interest to know the above data in his possession

you can take further action if you believe your personal information has been misused.

Applicant 1 must make the sound recordings unrecognizable to the original subscribers

the place and time of birth and the name of their mother, unless they are the same as the recipient of the subscription with the name of the mother given by the person - but no other changes to the sound recordings can perform. As a result of the misleading information provided to the Applicant 1, that Applicant 1 does not process the Applicant's personal data - the Applicant does not presumed that in its application to the Authority it was necessary and worthwhile to You are requesting an obligation to fulfill 1 access request.

(71) III.3.2. The Authority grants the Applicant's request and Article 58 (2) (b) GDPR condemns Applicant 2 for violating Article 5 (2) of the GDPR;

ex officio in accordance with Article 58 (2) (g) of the GDPR order the restriction of the processing of the Applicant's personal data until Applicant 2 certify that the legitimate interest in data processing takes precedence over the rights of the Applicant and as he did not prove to the Authority in the course of the proceedings that he had those interests weighed and offset between.

(72) III.3.3. The Authority examined of its own motion whether it was justified in respect of the Applicants imposition of a data protection fine. In this context, the Authority will comply with Article 83 (2) of the GDPR and Infotv. 75 / A. § considered all the circumstances of the case and found that a in the case of infringements detected in the present proceedings, the warning is neither proportionate nor appropriate

a dissuasive sanction, it is therefore necessary to impose a fine. The Authority shall impose a fine the following factors were taken into account:

(73) III.3.3.1. The Authority took into account that the infringements committed by Applicant 1 a Constitute a more serious infringement under Article 83 (5) (a) and (b) of the GDPR because the infringements committed by the Applicant 1 effectively and almost completely prevented and effectively made it impossible for the Applicant to exercise any control over your personal data.

(74) In imposing fines, the Authority assessed the following as aggravating circumstances:

 Applicant 1 acted with gross negligence when erroneously, contrary to reality

informed the Applicant that he does not process his personal data and to Applicant 2

without assessing which of its records, at what level

personal data of the Applicant is or may be included. Therefore, the

False information provided by Applicant 1 on the data processing was delayed by the Applicant

and limited its enforcement capacity.

 Applicant 1 also did not take any measures to ensure that a

Correct the misinformation given to the applicant and the one he actually handled

provide information to the Applicant.

 In its reply dated 29 January 2019, the applicant also informed the Authority that

does not process the Applicant 's personal data in its registration system and that

sent all available documents to the Authority. With this

provided information only on the repeated request of the Authority that the Eht.

With reference to Section 158 (1), which personal data does the Applicant handle?

he also attached to that reply sound recordings of the rewriting of the contracts, of which

as a result, the infringement did not cooperate with the Authority to the extent expected

to investigate and remedy.

(75) The Authority assessed as a mitigating circumstance that the general obligation to convict

has not yet taken place due to a breach of the Data Protection Regulation.

(76) The imposition of a fine is necessary in respect of Applicant 1 specifically or similarly

data controllers in order to prevent further infringements

despite the fact that it relates to the exercise of the rights of a single data subject in the present case

it is an infringement.

(77) In view of the above and the fact that Applicant 1 is according to its 2017 accounts

sales revenue was more than HUF 72 billion, the data protection fine imposed is a symbolic

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

(78) The amount of the fine was determined by the Authority in the exercise of its statutory discretion

me.

(79) III.3.3.2. The Authority first of all took into account that it was committed by the Applicant 2

infringements constitute a more serious infringement within the meaning of Article 83 (5) (a) and (b) of the GDPR.

as there has been a clear breach of the data protection principle and

handled the Applicant's personal data on the basis of an inappropriate legal basis.

(80) In setting the fine, the Authority assessed the following as attenuating circumstances:

16

 The processing of data requested on the basis of 2 inappropriate legal bases is inappropriate

resulting from its legal interpretation.

 Debtor 2 withdrew the ongoing enforcement proceedings that a

Initiated against the applicant, based on the above data management.

 Requested 2 took measures to prevent this from happening in the future

to handle the number of identity documents.

(81) In view of the above and in view of the fact that the Applicant has submitted its 2017 accounts

sales of nearly seven and a half billion forints, the imposed data protection fine does not exceed

maximum fine that may be imposed.

(82) III.3.4. The Authority rejected the Applicant's request to bind the Applicants

to delete your personal data, as Applicants have a legal basis for personal

to manage your data.

(83) III.3.5. The Authority rejected the Applicant 's request to ban the Applicants from the

processing of personal data, as the Authority in the data protection authority proceedings against the GDPR

It may apply the legal consequences provided for in Article 58 (2). The GDPR 58.

Article 2 (2) does not empower supervisory authorities to:

prohibit data controllers from processing the personal data of a specific data subject.

(84) On the basis of the above, the Authority has decided in accordance with the operative part.

(85) IV. Other issues:

(86) The powers of the Authority are limited to Infotv. Section 38 (2) and (2a), its jurisdiction is

covers the whole country.

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

Ákr. Pursuant to Section 82 (1), it becomes final upon its communication. The Ákr. § 112 and § 116

(1) and § 114 (1), the decision is administrative

there is a right of appeal.

** *

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

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

The administrative lawsuit against the decision of the Criminal Court falls within the jurisdiction of the court. § 13

(11), the Metropolitan Court has exclusive jurisdiction. The civilian

CXXX of 2016 on the organization of litigation. Act (hereinafter: Pp.) - the Kp. Section 26 (1)

applicable within the jurisdiction of the General Court pursuant to § 72

legal representation is mandatory in litigation. Kp. According to Section 39 (6) - unless otherwise provided by law

the bringing of the action for the administrative act to take effect

has no suspensive effect.

(89) A Kp. Section 29 (1) and with this regard Pp. Applicable pursuant to Section 604, the

of 2015 on the general rules of electronic administration and trust services

CCXXII. Pursuant to Section 9 (1) (b) of the Act (hereinafter: the E-Administration Act)

the client's legal representative is obliged to communicate electronically.

(90) The time and place of the application are set out in Kp. Section 39 (1). THE

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

based on paragraph The rate of the fee for an administrative lawsuit is set out in the 1990 Fees Act

XCIII. Act (hereinafter: Itv.) 45 / A. § (1). The fee is preliminary

from the payment of the Itv. Section 59 (1) and Section 62 (1) (h) exempt

initiating proceedings.

(91) If the Applicant does not duly demonstrate the fulfillment of the required obligation, the

The Authority considers that it has not complied with the obligation within the time limit. The Ákr. Section 132

if the debtor has not complied with the obligation contained in the final decision of the authority,

the executable. The decision of the Authority With the communication pursuant to Section 82 (1)

it becomes final. The Ákr. The Ákr. Section 133 enforcement - if you are a law

Government decree does not provide otherwise - it is ordered by the decision-making authority. The Ákr. 134.

§ pursuant to the implementation - if by law, government decree or municipal authority

In this case, the decree of the local government does not provide otherwise - the state tax authority

implements. Infotv. Pursuant to Section 60 (7) of the Authority,

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

with regard to the standstill obligation, the enforcement of the decision shall be:

Authority.

Budapest, April 17, 2019

Dr. Attila Péterfalvi

President

c. professor