Case number: NAIH / 2020/2074/2.

History: NAIH / 2019/1360.

NAIH / 2018/6733.

Subject: Rejection of the applicant's application

decision

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

at the request of the applicant (hereinafter referred to as the Applicant) against […] (hereinafter referred to as the Applicant)

In the data protection authority proceedings initiated on November 9, 2018, he made the following

Decision

The Authority shall reject the application.

The Authority finds that it has exceeded the administrative deadline and therefore HUF 10,000, ie ten thousand

HUF to the Applicant, at his choice, by bank transfer or postal order

to pay.

There is no administrative remedy against the Authority's decision, but a

within 30 days of the communication to the Metropolitan Court

may be challenged in an administrative action. The application must be submitted to the Authority

electronically, which forwards it to the court together with the case file. To hold a trial

the application must be indicated in the application. Those who do not benefit from full personal exemption

The fee for the administrative lawsuit is HUF 30,000, and the lawsuit is subject to the right to record material fees. THE

Legal representation is mandatory in proceedings before the Metropolitan Court.

EXPLANATORY STATEMENT

I. Procedure and clarification of the facts

I.1.The applicant received the application by post on 8 November 2018

initiated a data protection authority proceeding.

In this, the Applicant explained that his employment with the Applicant had been terminated

October 08, 2018. Job created on the day of termination in the handover protocol a

Applicant requested from Applicant that the computer provided for exclusive use

(special, medical and biometric) personal data

for. The Applicant further stated that he had not complied with the

He applied for the exercise of his rights as a data subject.

The Applicant also stated that he had become aware of a fact that for him

your data on a computer provided for your exclusive use without your consent

viewed, made multiple copies and used illegally. The Applicant

claims that your private mail has been made available through a password saved by your computer

for unauthorized persons.

The Applicant's request for an official data protection procedure is a right of access,

and the refusal to grant the data subject's request for cancellation,

and sought to establish the unlawfulness of the processing of his personal data

the Authority to instruct the Applicant on the basis of the right of access and cancellation

to comply with your request.

It can be stated from the attached documents of the Applicant that it was made at the time of his termination

in the minutes dated 8 October 2018 and again on 15 October 2018

requested that his personal data be made available and that they be deleted and made inaccessible

item.

Act CXII of 2011 on the right to information self-determination and freedom of information. law

(hereinafter: the Information Act) the right to the protection of personal data pursuant to Section 60 (1)

the Authority shall, at the request of the data subject,

initiated proceedings.

The Applicant, dated 10 December 2018, sent to the Authority for a rectification request,

stated in his statement that the Applicant had still not fulfilled the rights of the data subject

request for the exercise of that right.

The Authority issued a decision on the initiation of the data protection authority procedure NAIH / 2019/1360. case number

notified the Applicant in his order, at the same time providing information in order to clarify the facts

requested from the Applicant. By letter dated 18 February 2019, the Applicant shall issue this notice

(Declaration No 1 of the applicant).

The Authority considered that the applicant's further statements were clarified

necessary, so the first information in the Authority's proceedings during the procedure

at his request, he called for a statement three more times (March 29, May 8, and June 27, 2019)

the Applicant.

I.2. Statement by the applicant concerning ongoing litigation

In his statement No. 1, the Applicant stated that the Applicant had initiated proceedings before the Authority

On 24 October 2018, the Applicant filed an action in connection with the subject matter of

defendant against the Central District Court of Pest (hereinafter: the Court). The Court of Justice of […]

Ordered the referral of the application to the Metropolitan Court. The transmission

Order No. […] became final on 28 November 2018. By the Applicant

referred to and attached […] no. order for damages initiated by the Applicant

refers to the initiation of proceedings for the establishment of

The Applicant sent a copy of the order to the Authority. The Applicant is

CL of 2016 on general administrative order. Section 48 (1) of the Act (hereinafter: the Act)

with reference to paragraph 1 (a), according to which the authority shall suspend the proceedings if it:

a preliminary ruling falls within the jurisdiction of a court, requested that the proceedings of the Authority be stayed. THE

According to the petitioner, the litigation concerns the official data protection procedure

is considered a preliminary issue, so based on this, the Ákr. Pursuant to Section 48 (1) (a) of the Data Protection Act

there is a need to suspend official proceedings.

In addition to the above, the Applicant commented on the questions asked by the Authority as follows.

I.3.Claimer's first application

“The job dated October 08, 2018 in the handover protocol by the applicant “in the personal presence of your data and rights on your computer

[…] took note of his request for the complete deletion of his personal data,

did not contest the fulfillment of the request. […] Accordingly prepared the execution of the request for it

in accordance with Article 12 of the GDPR. in accordance with Article

exercise of their rights. Already after the application is submitted and the day after

provided an opportunity for […] to be in the applicant's personal presence and safe

under the conditions of data processing, the request of the applicant may be granted.

[…]

However, the above request of the applicant was impeded as the applicant did not

pursuant to Section 6 (2) of Act I of 2012 on the Labor Code - a

good faith procedural and cooperative activities necessary to implement the request

obligation, then

- when you refused to sign the privacy statements prepared by […], and

then

- when the applicant insisted on saving from the computer device himself

the data and not the […] IT officer to perform the backup operation ”

The Applicant In its statement, it stated that, in view of the fact that the computer was

It is “vital” for the performance of the Applicant’s duties, and therefore the Applicant is “legitimate

has an interest in backing up data from the device it owns to […] IT

carried out by a staff member. "

I.4. Applicant's second application (received on 17 October 2018)

The Applicant did not refuse to comply with the second request submitted by the Applicant,

but without undue delay, in a document dated 24 October 2018,

informed the person concerned of his measures. "In this he repeatedly asked […]

applicant

cooperation, in particular in favoring the implementation of the request

to agree on a date and the […]

office building application

appear in order to be achievable. "

According to the Applicant's statement, “[…] again in order to comply with the new application

failed to co - operate with […] 's administrative body, namely its legal representative in 2019.

did not contact […] to provide his details until the letter received on 30 January

and did not cooperate in any other way

in order to be achievable. "

I.5. Applicant's third application (filed on January 30, 2019, through its legal representative)

According to the statement of the legal representative, the legal basis for the issue is known to the parties

There was no dispute, so he merely requested that in addition to the Applicant 's personal appearance, the

Ensure the exercise of the right of access to the applicant's personal data and

requested information on whether a data protection incident or unjustified use occurred a

In connection with the personal data of the applicant. The Applicant is dated 18 February 2019

informed the Applicant's legal representative of the action taken on the application. THE

a copy of the letter was provided by the Applicant to the Authority.

According to the above information, the Applicant has not previously denied the application concerned

However, in his view, "In view of the

and in the data protection proceedings before the Authority, the burden of proof lies with […]

a pending situation has arisen with regard to the execution of the applicant's request.

The above pending situation is the […] official body of the National Data Protection and Freedom of Information

Also referred to it in a letter to the Authority, referring to Article 17 (2) (e) of the GDPR,

that the right to delete personal data does not apply if the data processing

to bring, assert or defend the necessary legal claims. "

I.6. In addition to the above, the Applicant informed the Authority that it could not declare that

what personal data is on the IT device because “The data for […]

could not be ascertained that it was actually placed on the device, given that

it would necessarily lead to access to the data, which […] is the sole responsibility of the applicant

lawful in his personal presence at the request and consent of the applicant

with attention."

The Applicant was taken back by the Applicant upon termination of the Applicant's employment

for the exclusive use of the computer with reference to the Labor Code

Section 80 (1) of Act I of 2012, on the basis of which the employee's employment relationship

upon termination, he is obliged to hand over his job in the prescribed manner and settle accounts with the employee.

According to the Applicant’s statement, “Prior to the anomaly involving […]

did not have internal rules on the use of IT tools, but […]

emphasizes that personal use of the IT device in your possession is personal

did not authorize the processing and the conditions for doing so - as in the Authority's prospectus

partition on your laptop's hard drive. "

I.7. On 14 March 2019, the Applicant forwarded to the Authority the application dated 1 March 2019.

a copy of the minutes made on the day of the application (hereinafter: the minutes), which is the Applicant

document the fulfillment of a request for access and deletion. According to the minutes:

The head of the applicant 's IT Office is in the sealed package (the applicant' s personal data

transferred to the Applicant’s courtroom.

At the request of the applicant's legal representative, the Requested Data Protection Officer shall provide a copy

on the day following the receipt of the computer device (2018).

the conditions for the rescue of the data on 9 October 2006 are set out below

according to.

“According to the minutes dated 9 October 2018, the applicant did not sign it. That's it

The cancellation measure was not implemented because the applicant refused to the signing of the protocol, by which […] was not authorized to delete the data, and therefore the

The applicant considered the original request to be […] terminated, in which the data was waived and

the applicant has requested that it be deleted. "

The Registrar has determined that the stamped paper of the device is intact,

and that, after the machine has been opened and switched on, it has been established that […]

profile was turned on.

The Applicant's legal representative asked the Applicant's administrator the following questions:

“Why didn’t BitLocker come in on this machine when we turned it on? - It is possible that

because the machine has not been turned off, as it will go to sleep when the lid is folded down.

Why does the profile under […] 's name appear when we turn it on? - Because when the applicant in the presence of the

the first data backup was attempted, performed with a domain admin, and to anyone who enters with a domain admin

brings up your profile. I indicate that I last saw this machine when the above data backup

we tried. ”

According to the Applicant, the computer was taken out of his office when it was switched on,

October 8, 2018 in the morning hours.

The Applicant and the IT staff viewed the event log on the machine (log file),

from which the IT professionals save the required data, then the Applicant and the Applicant

it was jointly established that all personal data requested by the applicant were relevant

was saved from the device, and the Applicant also saved the

activity data and then after the data is transferred to the device

the process of rescuing has been completed and the personal data requested by the Applicant to be deleted

have been irretrievably deleted.

I.8. The Authority referred to the Minutes sent by the Applicant on 14 March 2019

invited the Applicant to send to the Authority the Applicant's exclusive

handed over for use and then taken back by the Applicant upon termination of employment log files saved from the computer and inform the Authority that each

identifiers to whom it belongs in order to establish that it can be clearly identified

be who entered the computer and when. The Authority shall attach the same log files to the

He also asked the applicant in his order. The Authority requested those log files in order to

to find out whether the return of the computer device and the application of the data subject

whether they have entered or used it in the period between

The Applicant claimed that he could not send the log files to the Authority because it was

has not been handed over to him.

According to the statement sent by the Requested for the publication of the log files, the Requested

“Copied the log files for your own legitimate purposes” for your own legitimate purposes. The Applicant

following the request of the data subject for access and deletion, the Applicant considered that

that it is no longer necessary to store them, so you deleted them.

The Authority considered that a further statement by the Applicant was necessary, inter alia

to clarify what he based on the assumption that he no longer needed the

log files and why you no longer attached them with your Declaration No. 1, which states that

had to respond to the request and the supporting evidence

attach:

-

-

The computer handed over to the Applicant for exclusive use was made by the Applicant

after receiving the personal data on the IT device

and who used and stored them and how? What was the purpose of the data

use and storage? (Page 6)

Attach all copies of documents related to your answers that are

their claims are supported! (Page 8)

Above - NAIH / 2019/1360/6. According to the statement given by the Applicant, the

The assumption that it is no longer necessary to store log files was based on the assumption that

The Applicant stated in the Minutes that he had further claims against the Applicant

therefore, according to the Applicant, the storage of this data is not only necessary but, on the contrary,

would have been contrary to the general data protection rules. The Applicant also claimed that

with statement 1 did not attach the log files because they were not yet available at that time

the fulfillment of the data subject's request set out in the Protocol

they did not log on to the computer before.

According to the Applicant's statement, they can only access their own account on the other person's computer

users and can only log in with their own password. They could not enter the Applicant's computer

to enter at all, because the computer was physically separated, glued, unauthorized

was locked away, it is impossible to enter. The device is in the presence of the Applicant and the Applicant on it

after it was confirmed that the computer was locked, the data backup was open

as recorded in the Protocol… "

I.9. With reference to the Authority on 8 May 2019, the Applicant Section 5 (1)

wished to make further statements and comments ("comments"). The

In his comment, the Applicant emphasized that there was a fundamental disagreement with the Applicant

was that the Applicant did not agree to have it done in the presence of an IT professional

data retrieval, and this indicated a lack of cooperation from the Applicant, as the Applicant

he was aware that this was the only way to fulfill his request.

According to the Applicant's statement, the Applicant's consent was necessary for the

during the data backup, the personal data of the Applicant may be disclosed to the data subject, as the

In the opinion of the Applicant, the Applicant as an employer has no legitimate interest in this

may be related.

I.10. The Applicant shall submit to the Authority NAIH / 2019/1360/17. in his statement no

He explained that, in his view, the termination of the official data protection procedure had already taken place

After learning of the contents of the applicant's letter of 13 December 2019, it would have been justified, as a

According to the Applicant, the Applicant did not comply with the Authority's request to rectify the deficiencies.

I.11. The Applicant shall submit to the Authority NAIH / 2019/1360/18. in its statement of order no

He stated that, in his view, there was an obligation to delete the log files, since they had not

given that they contained the Applicant's personal data. Also about it

informed the Authority that on 1 March 2019, the date of fulfillment of the Applicant's request

has taken action to save the log files, which relate only to the date of execution of the request, and

it was for log files related to its execution, so they could only serve that purpose

as proof that the Applicant was logged into his computer on that day and the data was backed up

according to your request. According to the Claimant 's statement, the reason for saving the log files is

was that in the event that the Applicant might have reconsidered himself and the

He would have refused to complete the necessary statements according to the applicant, in which case a

Applicant could have proved that the data was saved as it can be seen from the log files

it would have been that the Applicant had entered the computer. As the Applicant was cooperative, therefore

the Applicant considered that it no longer had any interest or legal basis in preserving the log files.

I.12. The Applicant shall submit to the Authority NAIH / 2019/19. In its statement of order No

the Authority shall order the Applicant to pay a procedural fine with reference to Ákr. Section 64 (2)

referring to paragraph 1 of the judgment, since, in the applicant's view, 'during the proceedings

his statements did not advance the proceedings, but at the same time he made statements without evidence

it generated further unjustified calls, which led to an unjustified delay in the procedure. "

I.13. The Authority has issued NAIH / 2019/1360/21. s. [...] drawn up pursuant to [...]

of the Data Security Policy referred to in point [...] or any other such policy

of which the Requested Logging Procedure and the Log Entries

internal rules and regulations related to the content and retention period of log entries

identifiable. The Authority contacted the Applicant in order to verify that the

whether there were any internal regulations under which to decide this part of the application would have required the Applicant to store the required log data.

In its reply to the above call, the Applicant informed the Authority that “the internal

its data protection regulations do not contain any information related to the subject matter of this data protection authority

procedure

"and the provisions on data security are unjustified

as the applicant's request has already been proven to have been complied with ". The Authority

considered it necessary to get to know the Applicant in order to clarify the facts

data security policy, but found out that it was the case

does not contain any relevant provisions for its assessment.

In its statement, the Applicant requested the termination of the official procedure, and a

The Applicant's costs in the proceedings of the Applicant - ie in the amount of only HUF 12,400.

II. Applicable legal requirements

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

Article 2 (1) of Regulation (EU) 2016/679 (hereinafter referred to as the General Data Protection Regulation)

the General Data Protection Regulation applies to personal data in part or

fully automated processing of personal data and the processing of personal data

which are part of a registration system

which are intended to be part of a registration system.

Article 4 (2) of the General Data Protection Regulation "processing" means the processing of personal data or

any operation on automated or non - automated data files, or

a set of operations such as collecting, recording, organizing, segmenting, storing, or transforming

change, query, view, use, transmit, distribute or otherwise

harmonization or interconnection, restriction, deletion,

or destruction.

Personal data pursuant to Article 5 (1) (a) of the General Data Protection Regulation

must be handled lawfully and fairly and in a manner that is transparent to the data subject.

According to recital 39 of the General Data Protection Regulation, natural persons

how their personal data concerning them are collected,

how they are viewed or otherwise treated

the extent to which personal data are or will be processed.

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

shall be able to demonstrate such compliance

("Accountability").

Pursuant to Article 15 (3) of the General Data Protection Regulation, the controller is the controller

provide the data subject with a copy of the personal data By the person concerned

for additional copies requested, the controller shall be reasonable on the basis of administrative costs

may charge a fee. If the person concerned submitted the application electronically, the information shall be extensive

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

asks otherwise.

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

at the request of the controller, delete the personal data concerning him without undue delay,

and the data controller is obliged to make the personal data concerning the data subject unjustified

delete without delay if one of the following reasons exists:

(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 referred to in Article 6 (1) (a) or Article 9 (2)

(a) is the basis for the processing and there is no data processing

other legal basis;

(c) the data subject objects to the processing pursuant to Article 21 (1) and there is no overriding legitimate reason to process

the data or the data subject objects to the processing pursuant to Article 21 (2);

(d) personal data have been processed unlawfully;

(e) personal data are required by the law of the Union or Member State applicable to the controller must be deleted in order to fulfill an obligation;

(f) the collection of personal data through the information society referred to in Article 8 (1) in connection with the provision of related services.

Pursuant to Article 17 (2) of the General Data Protection Regulation, if the controller has disclosed personal data and is obliged to delete it pursuant to paragraph 1, the available taking into account technology and the cost of implementation steps, including technical measures, to provide the data that the data subject has requested them to provide the personal data in question deleting links or copies of such personal data.

Pursuant to Article 17 (3) of the General Data Protection Regulation, paragraphs 1 and 2 shall not apply if the processing is necessary:

(a) for the purpose of exercising the right to freedom of expression and information;

(b) the Union or Member State law applicable to the controller governing the processing of personal data for the performance of a task carried out in the public interest or in the exercise of a public authority conferred on the controller;

(c) in accordance with Article 9 (2) (h) and (i) and Article 9 (3), a on grounds of public interest in the field of public health;

(d) for the purposes of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, in accordance with Article 89 (1), where the processing referred to in paragraph 1 is likely to make such processing impossible or seriously jeopardize; obsession

e) to file, enforce or defend legal claims.

The Authority shall inform Infotv. With regard to Section 61 (1) (a), the General Data Protection Decree It may apply the consequences provided for in Article 58 (2).

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

Infotv. Pursuant to Section 38 (2), the Authority is responsible for the protection of personal data and the

monitoring the exercise of the right of access to data in the public interest and in the public interest

and facilitating the free movement of personal data within the European Union.

CL of 2016 on General Administrative Procedure. Pursuant to Section 112, Section 16 (1) and Section 114 (1) of the Act on the

there is a right of appeal through an administrative lawsuit.

Ákr. § 46 [Rejection of application]

The authority shall reject the application if:

(a) there is no statutory condition for instituting proceedings and this law does not

has no other legal consequences, or

(b) the application for enforcement of the same right has already been made by the court or authority

the content of the application and the applicable legislation have not changed.

The Ákr. Pursuant to the provisions of Section 6 (1) - (3), all participants in the proceedings are obliged

act in good faith and cooperate with other participants. Article 31 of the General Data Protection Regulation.

In the performance of the tasks of the controller and the processor, the supervisory

cooperate with the competent authority upon request. The General Data Protection Regulation.

Pursuant to Article 2 (2), the controller is responsible for ensuring that its processing complies with

data protection principles and must be able to demonstrate such compliance

The Ákr. According to Section 62 (1), if the available information is not sufficient for making a decision

data, the authority shall carry out an evidentiary procedure.

The Ákr. According to § 63, if the clarification of the facts so requires, the authority may invite the client to make a statement.

The Ákr. Pursuant to Section 64 (2), if the customer or his representative, despite his other knowledge, is

false statement or omission of material relevant to the case - not including if the witness does not

can be heard or the testimony of the Ákr. It is specified in Section 66 (3) (b) and (c) may refuse to do so - may be subject to a procedural fine.

The Ákr. Pursuant to Section 65 (1) and (2), the authority, if necessary during the clarification of the facts,

and the Eust. may require the customer to present a document or other document.

Pursuant to Article 58 (1) of the General Data Protection Regulation, the supervisory authority is investigating

acting, inter alia, from the controller in order to carry out its tasks

may request information and the controller shall give the supervisory authority access to the

all personal data and information necessary for the performance of his duties.

The Ákr. Pursuant to the relevant provision of Section 66 (3) in the present case, the making of a statement may be refused if

the statement of the client himself or herself is a criminal offense.

freedom of the press and the basic rules on media content.

a statutory media content provider (hereinafter: media content provider), or with it

employment or other employment relationship, even after the termination of the employment relationship, and

would reveal the identity of the person providing the information in connection with the activity.

The Ákr. Pursuant to Section 77, the authority is the one who breaches its obligation through no fault of its own

shall be required to reimburse the additional costs incurred or to be subject to a procedural fine. The minimum amount of the

procedural fine is occasionally ten thousand forints, the highest amount - unless otherwise provided by law.

in the case of a natural person, five hundred thousand forints, a legal person or other organization

HUF 1 million in the case of Article 58 (2) (i) of the General Data Protection Regulation

In the event of a breach of the obligation to provide access provided for in Article 58 (1), the Authority shall

higher - up to 4% of the total annual world market turnover for the previous financial year

may impose a fine on the controller or processor for all relevant cases

based on consideration of the circumstances.

III. Decisions of the Authority

III.1. Procedural issues

III.1.1. There was no need to reject the application as alleged by the Applicant, and

coupled […] no. order for proceedings for the determination of damages initiated by the Applicant therefore, it is substantiated that the making of the Applicant's statement

the court proceedings were pending at the time. For this reason, the Authority examined whether Ákr. 48.

Is there a condition for suspension pursuant to § (1) a).

The Ákr. There is no case of a preliminary question pursuant to Section 48 (1) (a). The Authority § 48

With reference to paragraph 1 (a), it may suspend its proceedings only if:

a well-founded decision cannot be made without considering the preliminary question.

In the present case, the subject of the official data protection proceedings is an issue which falls within the competence of the

Authority

with regard to Infotv. § 38 (2), therefore the suspension of the proceedings was not justified,

as the Authority has competence in matters concerning personal data, it is not

there is a case where a preliminary issue should have been dealt with in which the Authority has no decision

with authority. The court has the right to decide on the issue of damages, but this cannot be considered as such

preliminary issue of a data protection authority case.

III.1.2. The Ákr. With reference to Section 47 (1) (c), according to which the proceedings have become devoid of purpose,

the procedure was not terminated as it was objected to by the Applicant at the time of filing the application

data processing still existed, and the request is not limited to the deletion of personal data

order and fulfill the request for access, but the Applicant a

also requested the establishment of unlawful data processing, therefore the relevant part of the request was deleted and

after granting access, it had to be assessed on its merits by the Authority.

III.2. Applicant is personal

making it known

data

third

person

for

happened

unauthorized

According to the Applicant, his personal data stored on the computer is also for third parties

have become known and the Authority is therefore clarifying the facts in this respect

requested information and the attachment of log files from the Applicant.

In its statements, the Applicant informed the Authority that it was for the Applicant

the returned IT device was segregated and could not be accessed by unauthorized persons,

further emphasized that the computer was accessed only in the presence of the Applicant,

first, when the data subject's request has not been complied with because it is not cooperating

behaved and insisted that he be able to carry out the data rescue himself.

On my second occasion, they entered the computer on March 1, 2019, when they were successfully

the Applicant's request has been complied with.

The archiving of workstation data [...] is not required or required by law

The Applicant's own internal regulations do not contain any task or obligation. The access

and deletion following the execution of a request for cancellation will reveal the merits of that part of the request

made it impossible because the Applicant deleted the log files for the use of the computer, and

the deletion prevented full disclosure of the facts in this regard. For log files

deletion was made by the Applicant despite the legitimate interest in preserving them

and in the ongoing data protection authority proceedings

would have been necessary.

Due to the above, no evidence was obtained from the Applicant during the clarification of the facts

therefore the Authority cannot establish it in the absence of evidence

that unauthorized access to the Applicant 's personal data has occurred, therefore the

Authority rejects this request of the Applicant.

III.3. Facilitate the exercise of the data subject's request, violation of the right of access and deletion

question

Article 15 (3) of the Applicant's General Data Protection Regulation and the General Data Protection Regulation

In accordance with Article 17 of the Regulation, the Applicant shall comply with the General Data Protection Act

reply within a period of one month in accordance with Article 12 (3) of that Regulation

sent.

In its reply to the first and second requests from the data subject, the Applicant informed the Applicant that he would comply

with his request if the data protection

sign a declaration. The Applicant wished to execute the request in such a way that

computer scientist

the

Applicant

in the presence of

to view

the

informatics

tool

and perform operations in accordance with the Applicant's request on the personal data contained therein

data. According to the Applicant, the Applicant did not agree to this because he insisted

to exercise the rights of the data subject without the involvement of the IT person.

Data protection statement provided by the Applicant and made available to the Authority

By signing, the Applicant would have given his consent to the previously exclusive

personal data stored on a computer device provided for use by the employer's IT officer

in order to comply with the data subject's rights. With respect

that the Applicant stored his personal data on the IT device of his employer in such a way that

he did not receive explicit permission to do so, so he had to be aware of his personal information on the device

to charge that personal return in the event of any immediate return of the asset you can access your data with the help of other people. As the affected applications set

the Applicant was no longer employed by the Applicant on the date of performance of the

had to return the IT device in view of the terminated employment, therefore the

The Authority does not consider it objectionable that only the

the Applicant may have access to his / her personal data by a person authorized by his / her employer.

In the opinion of the Authority, the statement requested by the Applicant is from the Applicant Computer

It was not necessary to know the personal data stored on the device because

its completion in the given situation would not have substantiated the lawful acquaintance, data management,

due to the lack of voluntary consent in the present situation based on the legitimate interest of the Applicant

the personal data on the employer's device could, of course, only be disclosed to the extent strictly necessary. It should be

emphasized that the Candidate

as an employer, the legitimate interest does not explicitly relate to getting to know the former employee

personal information, but also to keep information related to its activities, secrets in its possession

stay. Work - related data stored on a computer device and

In order to separate the personal data of an employee, it is often essential to complete the device

which may also result in access to the personal data stored on it. THE

during the said computer scan, the Applicant provided adequate guarantees as it was only

IT and only in the presence of the Applicant.

In view of the above, the Authority concludes that the Applicant did not violate the General

Article 12 (2) of the Data Protection Regulation, as the Applicant assisted the data subject

exercise of the right of access and cancellation, not the right of access and cancellation of the Applicant

hindered because the conditions imposed by him were not excessive, but justified

in order to comply with the principle of accountability. Therefore, the Applicant

The Authority shall reject the relevant part of its application.

It was established from the Minutes that on 1 March 2019 the Applicant fulfilled the a

The applicant 's requests under the right of access and cancellation that in the personal presence of the Applicant, the Applicant's IT officer has entered earlier

took it back to a computer device and made a copy of the Applicant's personal data,

which he handed over to the Applicant and then deleted them from the IT device.

ARC. Other issues

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

whole

country.

The Ákr. Pursuant to § 112 and § 116 (1) and § 114 (1)

there is an administrative remedy against him.

***

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

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

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

The Metropolitan Court shall have exclusive jurisdiction pursuant to A Kp. Section 27 (1)

legal representation is mandatory in litigation 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 administration and trust services. Section 9 of the Act

Under paragraph 1 (b), the client's legal representative is required to communicate electronically.

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

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

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

Fees. law

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

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

During the procedure, the authority exceeded the Infotv. One hundred and twenty days in accordance with Section 60 / A (1)

administrative deadline, therefore Ákr. Pursuant to Section 51 b), it pays ten thousand forints to the Applicant.

Budapest, March 19, 2020

Dr. Attila Péterfalvi

President

c. professor