Case number: NAIH- 2868-23/2021.

Subject: decision approving the request

H A T A R O Z A T

Before the National Data Protection and Freedom of Information Authority (hereinafter: Authority) [...]

applicant (residential address: […]; hereinafter: Applicant) of his criminal personal data […] (residential address:

[…]; the

hereinafter: Submitted on the subject of illegal forwarding by the Respondent, a

It was received by the authority on February 23, 2021, and started on July 6, 2021 following its supplemented application

In an official data protection procedure, the Authority makes the following decisions:

I. The Authority grants the Applicant's requests and determines that the Applicant

I.1. violated the

processing of personal data for natural persons

regarding its protection and the free flow of such data, as well as a

on the repeal of Regulation 95/46/EC, the European Parliament and

Council 2016/679. (hereinafter: GDPR) Article 5 (1) paragraph a)

the principle of legal and fair data management according to point;

I.2. has violated the purpose of Article 5 (1) b) of the GDPR

principle of data management;

I.3. violated Article 6 (1) and Article 9 (1) of the GDPR.

II. The Authority ex officio, due to the violations established in point I, the Petitioner

300,000 HUF, i.e. three hundred thousand forints

data protection fine

obligates to pay within 30 days from the date of this decision becoming final

* * *

There is no place for administrative appeal against this decision, but from the announcement

within 30 days from the date of issue, with a letter of claim addressed to the Capital Tribunal

can be challenged in a lawsuit. The statement of claim must be submitted electronically to the Authority, which

forwards it to the court together with the case documents. Not in the full personal tax exemption

for beneficiaries, the fee for the administrative lawsuit is HUF 30,000, subject to the right to record the fee subject to the lawsuit

it's raining Legal representation is mandatory in proceedings before the Metropolitan Court.

I N D O C O L A S

I. Procedure of the procedure

(1) The representative of the Applicant certified with a power of attorney, [...] by post to the data protection authority

submitted a request for a procedure, which was received by the Authority on February 23, 2021.

(2) In his application for the data protection authority procedure, the Applicant asked the Authority to

determine that the Applicant's criminal personal data 2021.

unauthorized on January 6, or based on the application supplement on June 11, 2021

sending or making it available to persons is illegal

carried out data management in violation of Article 5 (1) of the General Data Protection Regulation

points a) and b) of paragraph 2, and the provisions of paragraphs (1)-(2) of Article 9. The Applicant

also requested that the Authority of the criminal personal data of unauthorized persons

……

1055 Budapest

Falk Miksa utca 9-11

Phone: +36 1 391-1400

Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu

www.naih.hu

by sending it to or making it available is illegal

due to data processing against the Requester, which is proportionate to the severity of the violation

impose a data protection fine.

(3) The Authority NAIH-2868-2/2021. No., dated March 12, 2021

the Requested, that the data processing carried out by him based on the Requester's request

a data protection official procedure was initiated to investigate its legality, and the facts

invited him to make a statement in order to clarify. The Applicant shall comply with the Authority's order in 2021.

received on March 26.

(4) At the same time, in order to clarify the facts, the Authority considered it necessary that

CL of 2016 on the general administrative procedure. Act § 25 (1) paragraph b)

on the basis of point, contact the Pest Central District Court (a

hereinafter: PKKB), and […] (hereinafter: […][Company]). The company]

statement was received on April 1, 2021, PKKB's statement on April 15, 2021

To authority.

(5) The Applicant dated 30 March 2021, at the seat of the Authority on 1 April 2021

in his personally submitted statement - NAIH-2868-6/2021. - asked in addition to his last name

the private handling of his personal data, since according to his statement he did not know how at that time

who is the requesting client in the procedure. In the same submission of the Respondent

also applied to the Authority with a document inspection request. The Applicant on this, NAIH-2868-

6/2021. in addition to his submission, he filed another submission on April 1, 2021

submitted personally to the Authority – NAIH-2868-7/2021.–, in which the Authority

the

deadline

he requested an extension in such a way that the 15-day deadline is his document inspection request

based on the date of receipt of the copies of the documents provided,

furthermore, he withdrew his request for private processing of his personal data.

to make a statement

fact finder

in its execution

provided

the

(6) The Authority NAIH-2868-9/2021. the Requested document inspection issued an order at no

on the limitation of his right, in view of the fact that one of the attachments of the [Company's] submission

according to the statement of the [Company], it was a trade secret, so the Authority does not

could provide access to the Applicant. Beyond that, however, everything else

a copy of the document created in the case, not received by him or not sent to him a

He made it available to the applicant. The Respondent restricts his right to inspect documents

he did not exercise any legal remedy against the order.

(7) The Authority accepted the request for extension of the requested deadline in NAIH-2868-10/2021. number,

He rejected it by order dated April 19, 2021.

(8) Statement of the Requested Fact-Checker by e-mail on May 6, 2021

arrived at the Authority, and then the Respondent submitted it personally to the Authority

at its headquarters on May 11, 2021.

(9) On July 6, 2021, through its legal representative, the Applicant supplemented the data protection

his request for an official procedure, since after submitting the request to the Authority a

He requested a new, previously complained about behavior to the detriment of the Applicant

carried out an identical act on June 11, 2021. For this reason, he asked

that the Authority applies the previously requested legal consequences to this data management

also applies in relation to activities.

(10) The Authority NAIH-2868-13/2021. No., dated July 22, 2021, notified the

Requested to supplement the application and to clarify the facts

asked him questions. The order sent to the Respondent by post is not sent by the post office

marked as wanted on August 11, 2021, the shipment on August 13, 2021

returned to the Authority.

2

(11) On August 12, 2021, the Applicant personally inspected documents at the Authority's headquarters

submitted a request to the Authority, or requested that the Authority send it to him again

NAIH-2868-13/2021. order no., which he failed to receive, since 2021.

on August 10, according to his statement, he did not get to the post office.

(12) After that, the Authority attempts to deliver its order to the Respondent again

for, he mailed it again on August 25, 2021, which the Requested 2021.

received on September 13, the 5th working day after the second notification.

(13) The Authority's document inspection request of the Respondent is NAIH-2868-15/2021. No. 2021.

in its ruling dated August 13, it was approved, which the Respondent is also the second

received on September 6, 2021, on the 5th working day after posting the notice, after

that day, he personally submitted another document inspection request to the Authority in the case.

(14) The Respondent, at the time provided for inspection of the documents, September 7, 2021-

I in the documents published at the Authority's headquarters, accessible to the proceedings

inspected and received a copy of NAIH-2868-4/2021, NAIH-2868-5/2021 and NAIH-2868-

12/2021. about the documents registered, and also made a statement in connection with the case,

which was recorded in the minutes of document inspection.

(15) The Applicant is NAIH-3868-13/2021. 2021 of the invitation contained in order no.

on September 29, in a statement submitted personally at the Authority's headquarters

enough.

(16) The Authority NAIH-2868-19/2021. No., dated October 26, 2021

informed the Applicant that he had completed the evidentiary procedure that had arisen in the case

you can look into documents, make a statement or request additional evidence. THE

by invitation, the legal representative of the Applicant, […] on November 2, 2021, document inspection

submitted an application to the Authority, to which the Authority granted NAIH-2868-21/2021. number,

He agreed with his order dated November 4, 2021. The Applicant's legal representative a

his statement based on the documents provided to him was received on November 17, 2021

For strength.

II. Fact

(17) With his report dated April 1, 2020, the Respondent initiated private criminal proceedings

initiated against the Applicant as a private person - who is the [Company]

legal advisor - before the PKKB. The Respondent submitted in his report that the Applicant

as the [Company's] legal advisor, he was transferred by the other two in the case without authorization and without reason

his defendant's "strict private secret", which was a private letter from the president and vice president of [...]

towards.

(18) On the basis of the report, criminal proceedings were initiated for violation of privacy, which is the first time

it was filed under [...] number, and later under [...] case number. PKKB on the criminal procedure

solo 2017 XC. based on Section 768 (1) of the Act, scheduled a personal hearing

who attempted to subpoena the Applicant as a declarant. Given that the

The wrong address was entered in PKKB's records, the summons is addressed to the Applicant

delivery was unsuccessful, with the indication "address cannot be identified" December 14, 2020-

I was sent back to the PKKB. The PKKB is attached to the request of the Authority

on the basis of a copy of the return receipt

repeatedly attempted to deliver the

For an applicant to another address in December 2020, however, on January 18, 2021

came back to the PKKB with a no-look signal.

subpoena

(19) In this regard, the Applicant emphasized that the incorrect address - [...] - was provided by the Respondent

provided in his report as the Applicant's residential address, even though the report was filed

on - April 1, 2020 - the address of the Applicant's new place of residence to anyone

was already included in the company register, which is available free of charge, given that the

According to the company copy of [Company], the change will be registered on October 23, 2019

cost. Consequently, according to his point of view, it can be reasonably assumed that the Respondent

despite the fact that he indicated […] as the Applicant's residential address in the report

was aware of the change of the Applicant's address.

(20) According to the Respondent's statement, 2021.

on January 5

viewed by him

initiated criminal proceedings, where he took a photograph of the Applicant

about the subpoena and the unopened envelope. After the Respondent became aware of this

about the failure to deliver the summons to the Applicant, the summons and the

took a photograph of an envelope containing an undelivered summons on January 6, 2021

At 0:40, it was sent by e-mail to [...] - the [Company's legal representative

law firm]'s lawyer -, for [...] - the [Company's] chamber legal adviser -, for [...] - the

An employee of [Company] -, to [...] - the chairman of the board of [Company] -, to [...] - the

Member of the supervisory board of [Company] -, for […] - employee of [Company] -, […]-

nak - an employee of the [Company] - and to the [...] e-mail address.

(21) Based on the introductory part of the summons - "The court for the offense of breach of privacy

[...] and his companions in the criminal case (...) [Applicant] is cited as a defendant." – the e-

it became clear to the email recipients that the Applicant was affected by the subpoena

participates as a defendant in a criminal case. According to the Applicant's position in the subpoena

in addition to the contents, the e-mail itself also contains numerous criminal charges relating to the Applicant

contained personal information: “[Applicant] due to a breach of privacy

appeared as a defendant in a criminal case at the PKKB on […] at […] in the courtroom […]

has an obligation." The Respondent stated in the e-mail that he is sending the letter for the reason

that the Applicant "should not be able to evade his criminal liability, nor

attempt, and the aim is also to make the procedure to [the Applicant] and the other [Companies]

not be able to drag away the related load.”

(22) According to the Applicant's statement submitted in his request for official data protection procedure

the [...] e-mail address is the central e-mail address of the [Company], therefore 142 people have access to it to his knowledge. The [Company] dated March 29, 2021, in response to the Authority's request in his statement, he informed the Authority that at the time of making the statement, [...] e-mail address was accessed by 147 people, the number of which varies. Declaration of the Applicant on July 5, 2021, the number of people with access was 216. The e-mail the account is accessed by [...] consultants, complaint handling staff, [...] staff, etc. In contrast, the Respondent believes that only two people have access to the e-mail account, however, he did not substantiate this claim with anything.

(23) According to the Respondent, other than the Applicant's name and address are personal did not send his data to the central e-mail address of [Company], and also explained that a transmitted personal data were known to the [Company], as well as the meetings of the PKKB are also public.

(24) According to the Respondent's statement, the purpose of the data transmission was that the Applicant make sure to appear at the hearing scheduled for [...] and that the case does not drag on. THE The Respondent does not have the Applicant's e-mail address - according to his statement, there are more he also tried a variation - so he couldn't send him directly about the summons took a photo. According to the Respondent's statement, the Applicant is on trial its appearance was only due to his letter. In support of this, he attached a minutes of a personal hearing held on January 11, 2021, which according to the Applicant stated that "I did not receive the summons, but the victim informed about the meeting."

(25) He further explained that the e-mail was also a message to the [Company], that is "it also served as a complaint and I sounded the alarm to the [Company] that they should start operate legally. The other goal was [the Applicant's] appearance at the PKKB. Both goals fulfilled." The Applicant also submitted that his letter also served the purpose of a complaint, therefore

legally sent your letter to […] e-mail address, which is the official [Company].

complaint handling e-mail address.

(26) With the Respondent's complaint dated September 11, 2020, against the Applicant

another private prosecution was initiated at the PKKB for breach of privacy

due to which it was first filed at [...] number and then at [...] number. PKKB in this

also a personal hearing in the case

pinned on which the Applicant

tried to summon him as a declarant. The Respondent, as in the previous case, when

became aware of the failure to serve the summons, addressed to himself

summons, as well as the summons addressed to the interpreter also summoned for the personal hearing

- from which, according to the Applicant's position, it is clear that the Respondent

criminal proceedings against the Applicant initiated by - June 2021

At 08.28 on the 11th, he sent it to third parties via e-mail. The recipients are a

were: […], chairman of the board of the [Company]; […], […], […] and the

Employees of [Company]; [...], the [Company's] legal counsel and [...], the Company

member of the supervisory board. The Respondent also sent this email to

Also to [Company]'s central e-mail address, […].

(27) According to the Applicant's point of view, the subpoenas were clear in this case as well

based on its introductory parts - "Due to the offense of violation of privacy of the court [a

in the criminal case against the Applicant] and his associates" - that the Applicant with the subpoena

participates as a defendant in the relevant criminal case. In addition, according to the Applicant's point of view, a

in addition to the subpoena sent as an attachment, the text of the e-mail also contained the

Criminal personal data concerning the applicant, according to "[…]"

(28) In connection with his electronic letter written on June 11, 2021, the Respondent submitted that with

sent the summons to the recipients of the e-mail with the aim that the Applicant is the personal one

to appear at the hearing, as the Applicant never receives it at his official address

citation. In his opinion, the Applicant is sabotaging all court proceedings by

he deliberately does not accept subpoenas, while his goal as a private prosecutor is to

to prevent "this […]" and to inform him of his obligation to appear in this way

the Applicant.

(29) To the questions of the Authority, for what purpose and on what legal basis the Applicant handled

his personal data related to criminal cases, declared that he is not a data controller.

(30) The Respondent made during the exercise of his right to inspect documents, NAIH-2868-17/2021.

he requested in his statement recorded in protocol no

external termination in view of the fact that the Applicant did not contact him in any way

with a "data protection request", even though, according to his point of view, the request was based on data protection

the prerequisite for initiating official proceedings.

(31) He also requested the termination of the procedure on the grounds that his data processing did not go beyond the

for personal purposes, sending e-mail did not exceed your personal activity.

Furthermore, according to his position, Infotv. rules apply,

in view of the fact that he acts as a private prosecutor in the above criminal cases, on the other hand, a

The applicant requests the Authority to determine the provisions of the GDPR. He noted

furthermore, in his opinion, the Authority, with the present procedure, is in conflict with Infotv

unfairly interferes with criminal proceedings.

(32) In its statement dated September 28, 2021, the Respondent also reiterated

his request for the termination of the procedure, in which the reason for the termination is a

in addition to the above, he also referred to the fact that the e-mail he sent did not contain the

Personal information about the applicant and his name were known to everyone.

(33) In addition, according to his point of view, there is also room for the termination of the procedure because

he is an individual, he is not a data controller, he does not have a data management information sheet, so neither does the

GDPR,

nor Infotv. its provisions do not apply to it.

III. Applicable legislation

so no professional or business

Recital (18) GDPR: This regulation does not apply to personal data a

carried out by a natural person exclusively in the context of personal or home activities

treatment which

cannot be brought by activity

in context. Personal or home activities include, for example, correspondence, a

address storage, as well as performed in the context of the aforementioned personal and home activities,

contact and online activities on social networks. We need this regulation

apply, however, to those data managers and data processors who are the personal data

the means for handling such personal or home activities

are provided.

GDPR Article 2 (1) and (2) points c) and d): (1) This regulation shall apply to

for processing personal data in a partially or fully automated manner, as well as

for the non-automated processing of personal data that

are part of a registration system or which are a registration system

want to be part of.

(2) This regulation does not apply to the processing of personal data if:

c) natural persons only in the context of their personal or home activities

carry out

d) prevention, investigation, detection and prosecution of crimes by the competent authorities

including the

carried out for the purpose of carrying out or enforcing criminal sanctions,

protection against threats to public safety and prevention of these threats.

GDPR Article 4, Point 2: "data management": automated on personal data or data files

or any action or set of actions performed in a non-automated manner, such as a

collection, recording, organization, segmentation, storage, transformation or change, query,

access, use, communication, transmission, distribution or other means

by item, coordination or connection, restriction, deletion or destruction;

Article 4, point 9 GDPR: "addressee": the natural or legal person, public authority,

agency or any other body with or with which the personal data is communicated,

regardless of whether it is a third party. Those public bodies that have a unique investigation

can access personal data in accordance with EU or Member State law,

are not considered recipients; the said data must be managed by these public bodies,

to comply with the applicable data protection rules in accordance with the purposes of data management;

GDPR Article 4, point 10: "third party": the natural or legal person, public authority,

agency or any other body that is not the same as the data subject, the data controller

with a data processor or the persons who are the data controller or data processor

were authorized to handle personal data under his direct control;

GDPR Article 5 (1) points a)-b): Personal data:

a) handling legally and fairly, as well as in a transparent manner for the data subject

must be carried out ("legality, due process and transparency");

b) it should be collected only for specific, clear and legal purposes, and not those

be treated in a manner inconsistent with these purposes; of Article 89 (1).

accordingly, the public interest is not considered incompatible with the original purpose

for archiving purposes, for scientific and historical research purposes or for statistical purposes

further data processing ("target binding");

Article 6 (1) GDPR: The processing of personal data is only lawful if and to the extent that

if at least one of the following is met:

a) the data subject has given his consent to the processing of his personal data for one or more specific purposes

for its treatment;

b) data management is necessary for the performance of a contract in which the data subject is one of the parties,

steps

or at the request of the data subject prior to the conclusion of the contract

necessary to do;

by

c) data management is necessary to fulfill the legal obligation of the data controller;

d) the data processing is for the vital interests of the data subject or another natural person

necessary for its protection;

e) the data management is in the public interest or for the exercise of public authority delegated to the data controller

necessary for the execution of the task carried out in the context of;

f) data management to enforce the legitimate interests of the data controller or a third party

necessary, unless the interests of the person concerned take precedence over these interests

interests or fundamental rights and freedoms that make personal data protection

necessary, especially if a child is involved.

Article 9 (1)-(2) GDPR: (1) Racial or ethnic origin, political opinion, religious

or personal data referring to worldview beliefs or trade union membership, and

genetic and biometric data aimed at the unique identification of natural persons, that is

health data and the

on the sexual life of natural persons or sexual

processing of personal data regarding your orientation is prohibited.

(2) Paragraph (1) does not apply in the event that

a) the data subject has given his express consent to one or more of the mentioned personal data

for its processing for a specific purpose, unless EU or member state law so requires

stipulates that the prohibition referred to in paragraph (1) cannot be lifted by the person concerned

with his consent;

b) data management means the employment of the data controller or the data subject, as well as a

regulating social security and social protection

arising

necessary for the fulfillment of its obligations and the exercise of its specific rights, if it is

EU country that also has adequate guarantees protecting the fundamental rights and interests of the person concerned

member state law or the collective agreement according to member state law makes this possible;

from legal regulations

c) data processing is for the vital interests of the data subject or other natural person

necessary for its protection, if not due to the physical or legal incapacity of the person concerned

able to give consent;

d) the data management is a foundation with political, ideological, religious or trade union purposes,

association or any other non-profit organization graduated under appropriate guarantees

takes place within the framework of its legal activities, on the condition that the data management

applies only to current or former members of such body, or to persons who

who are in regular contact with the organization in relation to the organization's goals,

and that personal data is not used without the consent of the data subjects

they do

accessible to persons outside the organization;

e) the data management refers to personal data that the data subject expressly requests

made public;

f) data management for the presentation, enforcement and protection of legal claims

necessary or when the courts are acting in their judicial capacity;

g) data management is necessary due to significant public interest, based on EU law or Member State law,

which is proportionate to the goal to be achieved, respects the protection of personal data

to ensure the essential content of the right and the fundamental rights and interests of the data subject

prescribes appropriate and specific measures;

h) data processing for preventive health or occupational health purposes, a
assessing the employee's ability to work, establishing a medical diagnosis,
provision of health or social care or treatment, or health or
necessary for the management of social systems and services, EU or
based on member state law or pursuant to a contract with a healthcare professional,
and subject to the conditions and guarantees mentioned in paragraph (3);
i) data management is necessary for reasons of public interest in the field of public health, such as a
protection against serious health threats that spread across borders or that
health care, medicines and medical devices are high
to ensure its quality and safety, and on the basis of EU or member state law
takes place, which provides for appropriate and specific measures for the rights of the data subject and
guarantees protecting your freedoms, and in particular regarding professional confidentiality;
j) data management in accordance with Article 89 (1) for the purpose of archiving in the public interest,
necessary for scientific and historical research or statistical purposes
or on the basis of Member State law, which is proportionate to the goal to be achieved, respects the
the essential content of the right to the protection of personal data, and the data subject is fundamental
prescribes appropriate and specific measures to ensure your rights and interests.
GDPR Article 77 Paragraph 1: Without prejudice to other administrative or judicial remedies,
all data subjects have the right to complain to a supervisory authority – in particular a
according to your usual place of residence, your place of work or the place of the alleged infringement
in a Member State - if, according to the judgment of the data subject, the processing of personal data relating to him
violates this regulation.
Infotv. Section 2, Paragraphs (2)-(4): Personal data are defined in accordance with (EU) 2016/679 of the European Parliament
and
under the scope of the Council Regulation (hereinafter: general data protection regulation).

the general data protection regulation in III-V. and VI/A. In Chapter, as well as Section 3, 3., 4., 6., 11.,

12., 13., 16., 17., 21., 23-24. point, paragraph (5) of § 4, § 5 (3)-(5), (7) and (8)

paragraph, paragraph (2) of § 13, § 23, § 25, § 25/G. § (3), (4) and (6)

in paragraph 25/H. in paragraph (2) of § 25/M. in paragraph (2) of § 25/N. in §, it is

51/A. in paragraph (1) of § 52-54. §, § 55 (1)-(2), § 56-60. in §, a

60/A. (1)-(3) and (6) of § 61, points a) and c) of § 61 (1), § 61 (2) and (3)

paragraph, paragraph (4) point b) and paragraphs (6)-(10), paragraphs 62-71. in §, § 72-

in, paragraphs (1)-(5) of § 75, § 75/A. § and defined in Annex 1

must be applied with supplements.

(3) This Act applies to the processing of personal data for law enforcement, national security and national defense purposes

should be used.

(4) For the processing of personal data not covered by paragraphs (2) and (3).

a) in Article 4, II-VI, and VIII-IX of the general data protection regulation. in the chapter, as well as

b) Sections III-V of this Act. and VI/A. In its chapter, in addition to § 3., 3., 4., 6., 11., 12., 13., 16., 17.,

21., 23-24. point, paragraph (5) of § 4, paragraphs (3)-(5), (7) and (8) of § 5,

in paragraph (2) of § 13, § 23, § 25, § 25/G. § (3), (4) and (6)

in paragraph 25/H. in paragraph (2) of § 25/M. in paragraph (2) of § 25/N. §-in,

the 51/A. in paragraph (1) of § 52-54. §, § 55 paragraphs (1) and (2), § 56

§ 60, 60/A. §§ (1)-(3) and (6), § 61 § (1) points a) and c)

in subsections (2) and (3), subsection (4) b) and subsections (6)-(10) of § 61, the

62-71. §, § 72, § 75 (1)-(5) and Annex 1

specific provisions must be applied.

Infotv. Section 3, point 4: criminal personal data: during or before criminal proceedings a

in connection with a crime or criminal proceedings, for the conduct of criminal proceedings,

and bodies authorized to detect crimes, as well as the execution of sentences

organization, which can be linked to the person concerned, as well as the criminal record

relevant personal data;

Infotv. Section 5 (7): In the case of criminal personal data processing - if it is a law, international

a contract or a binding legal act of the European Union does not provide otherwise - a

the rules regarding the conditions for handling special data must be applied.

Infotv. The right to the protection of personal data based on paragraphs (1) and (2) of § 60

in order to enforce it, the Authority is a data protection authority at the request of the data subject

initiates proceedings. Regarding the general administrative procedure for the official data protection procedure

2016 CL. Act (hereinafter: Act) shall be applied in Infotv

with specific additions and deviations according to the general data protection regulation. The

request to initiate a data protection authority procedure in Article 77 (1) of the GDPR

can be submitted in specific cases.

XC of 2017 on criminal proceedings. Act (hereinafter: Be.) Section 37: In criminal proceedings

the accused, the person who can be reasonably suspected of having committed the crime, the defender, a

injured party, the private plaintiff, the substitute private plaintiff, the private party, the property interested party, other interested

parties and

as defined by law, the legal entity subject to the procedure participates.

On. Section 39, paragraph (3) point a): The debtor is obliged

a) the court, the prosecutor's office and the investigative authority in procedural acts

to be present in accordance with the provisions of this law,

On. Section 53, paragraph (1) point a): The private plaintiff is the victim,

a) who commits light bodily harm, breach of privacy, breach of correspondence, defamation,

defamation, defamation or a false voice that is capable of defamation

in the case of taking a photo, he represents the prosecution,

provided that the offender

can be punished on private initiative.

On. § 98, paragraph (3): If the relevant legislation on the data subject does not provide otherwise,

the persons participating in the criminal proceedings are known based on the provisions of this law

personal data and protected data to exercise their rights or obligations under this law

they can handle it to the extent and for the time necessary for its performance.

On. § 112. Paragraph (2): Whoever is summoned must be summoned by the court, prosecutor's office or investigator

to appear before the authorities.

On. Section 116, subsection (1), point a): (1) If the subpoenaed party does not appear despite the summons, and

in advance, as soon as he becomes aware of the obstacle, he does not immediately rescue him, or if this is already the case

it is not possible, immediately after the obstacle is removed, he does not prove it with a valid reason,

a) the accused or the person who can be reasonably suspected of having committed the crime

leading or during the investigation of the accused or the commission of the crime

the production of a reasonably suspected person may be ordered,

and those listed must be obliged to compensate the criminal costs incurred.

On. § 130. Paragraph (1): The court, the prosecution and the investigative authority

a) by post,

b) electronically to the official contact information according to the E-Administration Act, or

contact information for secure electronic contact,

c) personally,

d) by announcement, or

e) through the delivery service of the court, the prosecutor's office or the investigative authority

delivered to the addressee.

CCXXXVII of 2013 on credit institutions and financial enterprises. law (a

hereinafter: Hpt.) Section 288, paragraph (1): The financial institution and the independent intermediary

ensures that the customer is aware of the behavior of the financial institution and the independent intermediary,

verbally (in person, on the phone) or

in writing (in person or through a document handed over by someone else, by post, by fax, electronically

by letter). The rules on complaint handling must be applied to a

also to a person who contacts a financial institution in order to use a service,

with an independent intermediary, but does not use the service.

ARC. Decision

IV.1. The Applicant's quality of data management, the types of personal data handled

(34) In his statements, the Respondent disputed that the two e-mails were personal

would have handled data, according to his point of view, it did not contain criminal personal data,

its data management remained within the limits of private data management, even if it was implemented

data management, then Infotv. and the rules of the GDPR must not be applied, because the two

in cases in which the person who sent the e-mails acts as a private prosecutor. As a result, the

The authority considers it necessary to determine whether data processing has taken place, that is the scope of the GDPR

whether it was subject to and what data it applied to.

(35) In the e-mail dated January 9, 2021, it was stated that the Respondent is sending the letter to

so that the Applicant "cannot evade his criminal liability" and "the procedure [the

[Applicant] and other [Company]-related debtors cannot be dragged away." Also about that

also informed the recipients that the Applicant "due to a violation of a private secret

appearing as a defendant in a criminal case at the PKKB on […] in the […] courtroom

has an obligation." The attached summons clearly states the case number

the subject of the case - the offense of violation of privacy - and the Applicant can be identified

procedural law position, according to which he is cited by the PKKB as a declarant. It was on the attached envelope

also a home address for which the summons from the PKKB was returned with an unidentifiable mark.

(36) In the text of the e-mail sent on June 11, 2021, it was stated that the Applicant did not take

through the "recent criminal court order addressed to him as a defendant, which is personal

cited with the burden of appearance", and it also contained that the Applicant was "burdened

in the case of breach of privacy". In addition, although the Respondent in his own name

attached a summons to his letter, it states the number and subject of the case, and that
the criminal case was initiated against the Applicant and his associates.
(37) Contrary to the Respondent's claim, his letters do not only contain the Applicant's name and address
included, but two additional ones relating to the Applicant that can be linked to him
also information related to pending criminal proceedings, such as
its procedural position in criminal proceedings, the nature of the crime. This data is
Infotv. They are classified as criminal personal data according to Section 3, point 4, since they are a
data generated during criminal proceedings. The Requested this data by e-mail
sent, forwarded to third parties, thereby performing data management, which
is considered a data controller, since he determined the method of data management - e-mail
sending - and its purpose, which is to deliver the summons to the Applicant, and a
The applicant had to appear at a personal hearing. The Authority is correct
considers the Applicant's application 2.2.3. its reference according to point, according to which
the person who is actually in charge of data management is considered a data controller
exerts influence, based on the above, this influence was concentrated at the Respondent,
as he decided and drove the transfer of the Applicant's criminal personal data
finally.
(38) As a result, the Requested Party is classified as a data controller, which it is not
is influenced by the fact that he is a natural person, since according to Article 4, point 7 of the GDPR
according to the definition, a data controller can be a natural or legal person. For this
in connection with this, the Authority notes that the Respondent's argument that, among other things
it is not a data controller because it does not have a data management information sheet, it is not correct, because it is
providing adequate information about data management is an obligation that is

it stems from the quality of the data controller, not the existence or lack of information
creates a person's data controller quality.

IV.2. Definition of the applicable legislation, the material scope of the GDPR

(39) After establishing that the Respondent acted as a data controller and

the subject of data processing was the Applicant's criminal personal data, it must

examine whether the GDPR, Infotv. – or the Applicant

according to him, neither - the applicable law.

(40) Article 2 of the GDPR defines the scope of the regulation, as well as Infotv. Section 2 (4)

paragraph also orders the GDPR to be applied to the data processing to which the

The scope of the GDPR would not be covered by the wording of Article 2 (1) of the GDPR

consequently,

and which do not qualify as personal data for law enforcement purposes,

its management for national security and national defense purposes. However, this provision

by definition, it does not override the provisions of Article 2 (2) of the GDPR, a

Exceptions to the scope of GDPR.

(41) In connection with the definition of the applicable law, taking into account the Infotv. Section 2 (4)

paragraph, as well as Article 2 (2) of the GDPR, it is also necessary to examine whether a

Can the data processing carried out by the respondent be considered as data processing for the purpose of law enforcement,

which he himself referred to - Infotv. does the data management fall under the scope of - and

if it is not classified as such, is it classified as private data processing which

does not fall under the scope of the GDPR.

(42) The Respondent referred to the fact that Infotv. falls under the scope of

because, based on his reports, two private criminal proceedings are also pending a

Against an applicant, in which he acts as a private plaintiff. The Be. Section 51, subsection (1) i)

point, the victim is entitled to act as a private plaintiff. The Be. According to § 37

the victim, or the victim acting as a private prosecutor, is a participant in the criminal proceedings

prosecutor's office, investigative authority, court. The Be. According to paragraph (3) of § 762 a

In addition to the rights of the victim, a private plaintiff is entitled to the rights associated with representing the prosecution. The

independent

rights of prosecution are only granted with regard to the accusation brought by him as the victim

the private prosecutor by not being able to exercise his official powers. 1 The accusation

as its representative, the private plaintiff within the framework of the private prosecution procedure regulated in Be

has the indictment and fulfills the role of the prosecutor exclusively in this respect. The

however, the prosecutor can take over the representation of the prosecution from the private prosecutor at any time.

says that it is

(43) The private prosecutor is therefore a victim without official powers. Article 2 (2) of the GDPR

point d) of paragraph specifically so

competent authorities

prevention, investigation, detection, prosecution of crimes or

data processing for the purpose of enforcing criminal sanctions is not covered by the GDPR

under its scope. As stated by the Metropolitan Court in 105.K.707.148/2020/15. no

pointed out in paragraph [22] of his judgment, this "rule is only the competence of the GDPR

applies to authorities, so the data management during which the

the authority (prosecutor's office or

court). In the present case, the nature of the investigated data management does not match the

with the facts of the judgment referred to, however, the Metropolitan Court on this

its finding is also relevant in the present case.

(44) Based on the above, therefore, by the Respondent, according to his position, in his capacity as a private prosecutor

data transmission carried out cannot be included according to Article 2 (2) point d) of the GDPR

under exception rule.

1 https://birosag.hu/sites/default/files/maganvadas_eljaras.pdf

(45) Subsequently, the Authority must also examine whether the Respondent is the Applicant

did you carry out the data processing objected to in the context of your personal or home activities.

Data processing carried out in the context of personal activity is to be interpreted narrowly, it is only and
it can only fall outside the scope of data protection regulations if it is exclusively for private purposes
serves. In that case, the data processing can no longer be considered for private purposes, if the purpose is
goes beyond private use, it is "directed outside the private sphere" as in
C-212/13. stated by the Court of Justice of the European Union in point 33 of the judgment. The Authority
his view is that if a private defendant in criminal proceedings as the private defendant
acting party, in this case the criminal personal data of the reported - Applicant
forwarded by a third party not involved in any role in the criminal proceedings
persons in order to achieve that the Applicant is the personal
appear at a hearing, it already extends beyond the scope of private use.

(46) According to the Authority's point of view, it could only then have been classified as the subject of the present procedure
sending two e-mails to data processing in the context of personal activity, if
the Respondent would have sent it directly to the Applicant only and exclusively.
However, considering that both e-mails, as well as the personal,
and criminal personal data to 7 people each, as well as to the Applicant's employer
he also sent it to a central [...] e-mail address, he overextended himself in the context of his personal activities
within the limits of data processing, so Article 2 (2) of the GDPR cannot be applied to its activities
exception according to paragraph c)

(47) Based on all of this, the Authority concludes that the Respondent investigated in this procedure
data processing falls under the scope of the GDPR.

such

(48) After that, the Authority examined the Respondent's objection that since a
The applicant did not contact it with a data protection request, therefore the Authority is in the case
cannot act, because it is a prerequisite for the Authority's procedure. However, Article 77 of the GDPR
does not define
condition, the parties involved are in advance with the data controller

regardless of contact, they are entitled to apply to the Authority if

in their opinion, the processing of personal data concerning them violates this regulation.

As a result, there is no condition defined by law, in the absence of which

in view of the fact that the application should have been rejected or later the procedure terminated

Acr. On the basis of § 46, paragraph (1) a) or § 47, paragraph (1) point a). As a result, the

This reference by the respondent is not acceptable, and the procedure cannot be terminated based on this

yes.

IV.3. Examination of the legality of data management

IV.3.1. Purpose-bound data management

(49) According to Article 5 (2) of the GDPR, the collection of personal data is limited to

it can be done for a clear and legitimate purpose, and they cannot be combined with these purposes

handle in a non-negotiable manner.

(50) The Be. According to paragraph (3) of § 98, the persons participating in the criminal proceedings - the Be. Section 37

according to such a person, both the victim and the private plaintiff - the Be. based on its provisions

learned personal data from the Be. to exercise their rights or their obligations under

they can handle it to the extent and for the time necessary for its performance. The Be. taking into account that the

during criminal proceedings, criminal personal data can typically be disclosed

participants, they may be treated by them, therefore the Be. this data is sensitive

in view of its nature, it determines for what purpose it can be processed legally, and what it cannot

other than Be. exercising rights or fulfilling obligations.

(51) The Respondent participates as a private plaintiff with the Applicant based on its reports

in criminal proceedings initiated against, i.e. represents the prosecution, and in addition to the rights of the victim, the

may exercise the rights associated with representing the prosecution, but may not extend beyond this.

As the Applicant also referred to in his application, the Be. Paragraph (1) of § 130

based on the delivery of official documents, including subpoenas, in private prosecution proceedings a

it is the court's task, not the victim's or the private plaintiff's.

(52) As a result, the private plaintiff, in this case the Respondent, cannot be taken over by the court

location in connection with the delivery of documents produced in private prosecution proceedings,

in the case of unsuccessful delivery, he is not entitled to the documents in an informal manner on his own authority

to be delivered to third parties, whether it reaches the cited person, or if

is also successful during informal delivery, it does not qualify in that case either

cannot be considered legally valid, i.e. the data processing carried out during such an act cannot be considered either

as legal.

(53) According to the Respondent's statement, the purpose of its data management was to

prevent the prolongation of the criminal proceedings and the Petitioner to appear a

in personal hearings for which

became. Prolongation of the procedure

prevention in private prosecution of the Be. however, not the private plaintiff,

rather, it is the task of the court, the defendant who does not appear for the summons can be summoned again by the court,

but, where applicable, you can also order it to be brought forward or produced.

quoted

(54) As a result, the Authority concludes that the data processing indicated by the Respondent

purpose cannot be considered legitimate in the Be. Based on § 98, paragraph (3), he therefore violated the

The principle of purpose-bound data management according to Article 5 (2) GDPR.

containing

also intended

they complain about your letter

(55) The Applicant also referred to the fact that, dated January 6, 2021, the Applicant

criminal personal data

so it is

the purpose of data processing was also to file a complaint. However, according to the Authority's opinion, the letter

meritorious, the Hpt. Not as a complaint in accordance with § 288, paragraph (1).

can be interpreted, it is not for the behavior, activities or omissions of the [Company].

concerned. The Respondent started his letter with the fact that the Applicant does not have the e-

with his email address, so he requests that "this official letter" be forwarded to him, and the letter is further

informs the recipients that the purpose of the letter is that the Applicant a

not be able to evade his criminal liability, or the "procedure [the Applicant] and the other

He cannot drag away a burden related to [the company]. Regarding [Company] only

all that is stated in his letter is that there are "data protection omissions" and [...], in addition

"the [Company] [...] will need internal due diligence, checks and investigations,

but about this […] I will send further information." Furthermore, as the subject of your letter

stated that "Send Summons where [Applicant] is the [Company] manager

his legal advisor is accused of a data protection crime, breach of privacy", i.e

when he sent the letter, he himself did not consider it a financial complaint, nothing indicating that

did not show. As a result, the Authority rejected the Applicant's argument that the letter

sending, and thus the transmission of the Applicant's personal data also for the purpose of handling complaints

served, does not consider it acceptable. According to the Authority's position, when the letter was sent

the Respondent had no intention of filing a complaint, it cannot be read at all from the letter

who, he only referred to later in order to justify his data management

legality.

IV.3.2. Legal basis for data management

(56) The Respondent did not respond to any of the Authority's invitations regarding the legal basis

forwarded the applicant's criminal personal data to third parties.

It should be noted that Infotv. Section 5 (7) for criminal personal data a

orders the application of the rules regarding the conditions for the processing of special data,

that is, subject to Article 9 (1) of the GDPR, the processing of criminal personal data

as a rule, it is prohibited and they can only be handled if the data management has a 6.

its legal basis according to paragraph (1) of Article, or one according to paragraph (2) of Article 9

condition exists.

13

(57) According to the Authority's point of view, in the specific case, only the legitimate interest of the Applicant, i.e

Article 6(1)(f) of the GDPR is the legal basis that can be applied,

with regard to that

also that the purpose of data management is initiated by him

marked the prevention of prolongation of criminal proceedings. Article 6 (1) GDPR

According to point f), the processing of personal data is legal if the data processing is carried out by the data controller

or is necessary to enforce the legitimate interests of a third party, unless on this

the interests or fundamental rights of the data subject take precedence over interests

and freedoms that require the protection of personal data. Especially

it is important that the data processing cannot refer to the legitimate interests of the data controller

disproportionate restriction on the rights and interests of the data subject.

(58) To be a data management

as its legal basis

be able to refer to it

for the legitimate interest of the data controller, in addition to identifying the legitimate interest, the data controller also

it must consider whether it is necessary to enforce the legitimate interest, that is

data controller must check whether they have an alternative

solutions, by means of which the legitimate interest can be asserted without data processing,

or with less restrictive means compared to the planned data management.

legally

(59) The Be. Pursuant to § 98, paragraph (3), the Respondent is the criminal proceedings initiated by him

in order to facilitate it, only those criminal matters that came to his attention during the procedure

is entitled to carry out actions related to the management of personal data, which offends him,

and is entitled or obliged based on his capacity as a private plaintiff, i.e. the Be. delimits the

scope of data processing that can be performed legally. The Applicant has expanded beyond this, as it is

Attempting to serve subpoenas, court documents on the Applicant is not his

task in criminal proceedings - especially not in such a way that criminal personal data a

forwards to third parties not involved in criminal proceedings - the omission

and the court is entitled to deduce its legal consequences.

not in the absence of authorization

(60) In addition, the data management chosen by the Respondent - in the text of e-mails and

transfer of criminal personal data contained in attached subpoenas – significantly

extended beyond the necessary extent by stating that in both cases seven, his report

to a person not participating in criminal proceedings, including the Applicant

to the central e-mail address of his colleagues or the Applicant's employer - to which

contrary to his unsubstantiated claim, not two, but 140-200

person has access to - forwarded the Applicant's criminal personal data, describing the

subject of criminal proceedings and the Applicant's procedural position. In this regard, the Applicant

submitted that, in his opinion, it is criminal personal data to learn about them

statutory

by

possibility if a

not even in the exceptional case

the defendant in a criminal case is in an unknown place and the Be. According to § 135 of the announcement

delivery becomes necessary. The Be. According to the commentaries attached to § 135

because "(...) the recipient's name may still appear in these announcements, but no longer,

in what capacity in the criminal proceedings, especially if you participate as a defendant, the be.

On the basis of § 98, paragraph (1), personal data in criminal proceedings, such as a

it is necessary to ensure the protection of criminal personal data." According to the Applicant, this

in light of this, not even the authorities and courts acting in criminal cases

his right to - if the document containing the criminal personal data a

it cannot be given to the recipient or to another person entitled to receive it under the law

deliver - in the notice with the addressee's position in criminal proceedings

include any related data, especially if the recipient is

participates in the proceedings as a defendant.

authorized persons

for

(61) In this context, the Applicant considered it necessary to also record that a

Criminal proceedings initiated by the Respondent affect the Applicant personally,

in them not as counsel or legal representative of the [Company] but

it was launched specifically as a result of the complaints made against him as a private individual

14

participates as a defendant in criminal cases, so not with his employer or his colleagues

it was justified to share your criminal personal data.

(62) Based on all this, the Authority came to the conclusion that the Respondent was not

did not have the legal basis for data processing according to Article 6 (1) of the GDPR, thus

investigating whether any of the circumstances under Article 9(2) of the GDPR

existed, unnecessary.

(63) Based on all of this, the Authority concludes that the Respondent is unlawful and compliant

in the absence of a legal basis, he forwarded the Applicant's criminal personal data to a third party

persons, in violation of Article 6 (1) and Article 9 (1) of the GDPR.

IV.3.3. The requirement of legal and fair data management

(64) According to the Applicant, the Respondent violated Article 5 (1) of the GDPR

the principle of legal and fair data management according to point a), since it is illegal, a legal basis

handled the Applicant's criminal personal data without In addition, it is

from the dishonoring and insulting style of e-mails sent, as well as the wide range of recipients

from the circle, it can be concluded that the Respondent's aim was no other than to

to portray the Applicant in a bad light in front of his colleagues and managers, furthermore,

that is accompanied by criminal proceedings initiated against the Applicant without grounds

out of frustration

unjustified

cause inconvenience with malicious intent.

unnecessary

in addition

further,

completely

and

too

(65) The fairness of data management is a requirement that, among other things, concerns the data subject

the right to self-determination of information, and through this to the private sphere, human

means respecting his dignity: the person concerned cannot become vulnerable to it

against a data controller or other person. The data subject during the process of data management

must always remain the subject of data management, cannot become a mere object of it.

(66) According to the Authority's point of view - examination of the intention and motivations of the Respondent

without - the e-mails sent, the criminal personal data contained in them third

transmission to persons was actually suitable for the Applicant

adversely affects his judgment in front of his colleagues. For this

regarding

it should be emphasized that the Respondent is not only the superiors and managers of the Applicant

sent the e-mails, who may have been aware that a

In contrast to the applicant as a private person, he was otherwise graduated in his job

in connection with his activities, the Respondent filed a report - NAIH-2868-6/2021. document number 1.

annex - but also to the […] e-mail address, to which a variable number of people, but a large number,

it can typically be accessed by employees performing customer service tasks who are not familiar with the

The background of criminal proceedings initiated by the respondent, i.e. in their case

e-mails were more apt to create a bad impression a

About the applicant. In this connection, it should be noted that the Applicant, in view of the Be.

according to the provisions referred to earlier, he could not expect that it was criminally personal

your data will be processed in this way, so you cannot take action or protest against it

known.

(67) Taking into account the provisions of the previous paragraph, as well as the fact that the Respondent

in the absence of a legitimate purpose, the Authority handled the Applicant's personal data without a legal basis

determines that it has violated the legality according to Article 5 (1) point a) of the GDPR

and the principle of fair data management.

IV.4. Request for the imposition of a data protection fine

(68) The Authority rejects the Applicant's request to impose a data protection fine.

The reason for this is, on the one hand, that since the application of this legal consequence is the right of the Applicant

his legitimate interest is not directly affected, for him such a decision of the Authority is a right

does not create an obligation, as a result, to enforce the public interest

application of legal consequence

regarding - the imposition of fines

falling within

regarding - the Applicant is not considered a customer under Art. Paragraph (1) of § 10

based on, so there is no place to submit an application in this regard, this part of the submission

cannot be interpreted as a request.

IV.5. Legal consequences

(69) The Authority grants the Applicant's request and determines that the Applicant

violated Article 5 (1) points a) and b) of the GDPR, Article 6 (1) and

paragraph 1 of Article 9.

(70) The Authority examined ex officio that

justified against the Application

imposing a data protection fine. In this context, the Authority is Article 83 (2) of the GDPR

considered all the circumstances of the case. Given the circumstances of the case a

The authority found that in the case of the violation discovered during this procedure - Infotv.

75/A. § - a warning is not a proportionate and dissuasive sanction, therefore

a fine must be imposed.

(71) The Authority took into account the aggravating circumstance when imposing the fine

the following:

•

•

•

•

•

their character

violations of law

assumed that

delivery to - was not

committed by the Respondent

considered more serious

are considered a violation of the GDPR Article 83 (5) point a) [GDPR

Article 83(1)(a)];

the purpose of data management of the Respondent - subpoenas through third parties

Applicant

legal, in the course of it

was overextended for him as a private plaintiff in the Be. provided by

rights [GDPR Article 83 (1) point a)];

forwarded by

the Applicant on both occasions to seven such people

Applicant's criminal personal data about whom

they know the

The applicant's contact information, even though to achieve the goal indicated by him - regardless

whether it was legal or not - it would have been enough for one person

send your letters. By sending it to the central email address of [Company].

and the Applicant made it known to a large number of additional employees

criminal personal data [GDPR Article 83 (2) point a) – data management

circle];

the Respondent initiated a number of official data protection procedures as a stakeholder

At the Authority, and against the Authority's decisions on several occasions in court

used a legal remedy, i.e. the Respondent can be said to be a data protectionist

is aware of issues, so his awareness should have understood that e-mails

sending it

commits an infringement, therefore according to the Authority's opinion

it can be established that the Respondent committed the violation intentionally. All this

is also supported by the fact that on June 11, 2021, the Applicant sent

another e-mail about the summons of the Applicant to a personal hearing by the court,

that you already knew that your email of January 6, 2021 with similar content

due to the request of the Applicant, a data protection official procedure is in progress [GDPR

Article 83(2)(b)];

the violation affected the Applicant's criminal personal data, which Infotv. 5.

(7) are considered special personal data [GDPR Article 83

(2) point (g)].

(72) During the imposition of the fine, the Authority took into account as a mitigating circumstance that a

The applicant is a natural person, also a job seeker, according to his declaration, he is regular

has no income [GDPR Article 83(2)(k)].

16

(73) The Authority did not consider GDPR Article 83 (2) relevant when imposing fines

circumstances according to paragraph d), e), f), h), i), j), since they are the specific case

cannot be interpreted in connection with

(74) On the basis of the above, the Authority made a decision in accordance with the statutory part.

A. Other questions

(75) The competence of the Authority is defined by Infotv. Paragraphs (2) and (2a) of § 38 define its jurisdiction

covers the entire territory of the country.

(76) The decision in Art. 80-81 § and Infotv. It is based on paragraph (1) of § 61. The decision is

Acr. Based on § 82, paragraph (1), it becomes final upon its publication.

(77) The Art. Based on § 112 and § 116, paragraph (1), and § 114, paragraph (1), the

against the decision and the termination order, there is an administrative lawsuit

as a remedy.

(78) The rules of administrative proceedings are laid down in Act I of 2017 on administrative proceedings

(hereinafter: Kp.) is determined. The Kp. Based on Section 12 (1), the Authority

the administrative lawsuit against his decision falls under the jurisdiction of the court, the lawsuit is referred to the Kp.

Pursuant to § 13, paragraph (3) point a) point aa), the Metropolitan Court exclusively

competent. The Kp. Under the jurisdiction of the court based on point b) of § 27, paragraph (1).

legal representation is mandatory in a lawsuit. The Kp. According to § 39, paragraph (6), the statement of claim

its submission does not have the effect of postponing the entry into force of the administrative act.

(79) The Kp. Paragraph (1) of § 29 and, in view of this, Pp. According to § 604, it is applicable

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

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

the client's legal representative is obliged to maintain electronic contact.

(80) The time and place of filing the statement of claim is determined by Kp. It is defined by § 39, paragraph (1).

Information about the possibility of a request to hold a hearing can be found in Kp. Section 77 (1)-(2)

based on paragraph

(81) The amount of the fee for the administrative lawsuit is determined by the XCIII of 1990 on fees. law

(hereinafter: Itv.) 45/A. Section (1) defines. Payment of the fee in advance

from under the Itv. Section 59 (1) and Section 62 (1) point h) exempt the procedure

initiating party.

Budapest, December 3, 2021

Dr. Attila Péterfalvi

president

c. professor