Case number: NAIH-937-1/2023. Subject: data protection initiated upon request

History: NAIH/2020/5689.

NAIH-435/2021

NAIH-462/2022.

decision in an official procedure

DECISION

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

[ ] (hereinafter: Applicant's representative)] represented by [ ] (hereinafter: Applicant)

at the request of the Budapest XI. District Police Department [(Address: 1518 Budapest, Pf.:13.)

(hereinafter referred to as: Respondent)] included in the decision No. [ ] made

in a data protection official procedure initiated in connection with the legality of the processing of data

makes the following decision:

I.

1. orders that within 8 days of receipt of this decision, the information

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

hereinafter: Infotv.) on the basis of point b) of § 17. Applicant - supplemented on June 25, 2020.

dated information - inform the Applicant as part of his right of access as to whether it happened

Data protection incident regarding the applicant's personal data, and with whom

was announced by No. [ ] dated May 21, 2020, subject "withdrawal of arrest warrant"

decision (hereinafter: Decision);

The Authority partially approves the request and

2. in the case of the Applicant, upon request, while in the case of the other affected victims/witnesses, ex officio

finds that the Respondent has violated Infotv. Paragraphs (1)-(2) and (4a) of § 4

with the fact that, in the absence of a legitimate purpose, it was unnecessarily recorded by the natural person

the name and delivery address of the parties involved as victims, as well as the delivery address of the Applicant

in the Decision;

3. the Authority grants the request and orders the final decision as Requested as

the disclosure by publication of the identification data of the data controller;

I.1. taking the measures prescribed in point, the Respondent from taking the measures

must be in writing within 8 days - with the submission of supporting evidence

together - certify to the Authority.

II.

The Authority issued the part of the application according to which the Applicant is the Applicant

communicated the decision to persons who were not entitled to know it,

and that the recording of the address of the Applicant's place of residence in the Decision violates it

the principle of purposefulness

rejects.

III.

The Authority ex officio determines that the Applicant during its procedure is the relevant

violated Infotv by failing to implement safety regulations. 25/I. in §

because it did not ensure the security of the witness' personal data, which was handled in private.

……

1055 Budapest

Falk Miksa utca 9-11

ugyfelszolgalat@naih.hu

www.naih.hu

Phone: +36 1 391-1400

Fax: +36 1 391-1410

ARC.

The Authority paid HUF 10,000, i.e. ten thousand forints, to the Applicant for administrative

due to exceeding the deadline - according to the choice of the Applicant to be notified in writing - to a bank account

pay by money order or postal order.

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 claim must be submitted to the Authority electronically, which

forwards it to the court together with the case files. In the full personal tax exemption

for non-beneficiaries, the administrative court fee is HUF 30,000, i.e. HUF thirty thousand

per subject is subject to the right to record levies. In the proceedings before the Metropolitan Court, the legal

representation is mandatory.

JUSTIFICATION

I. Facts, history

listed

It was initiated against the respondent for the crime of fraud committed in a businesslike manner, causing significant damage

criminal proceedings against the Applicant at [ ].

The applicant's representative submitted to the Authority on July 22, 2020

initiated a data protection official procedure against the Petitioner. performed by

that the Applicant sent the Decision to a total of 18 recipients. Among the recipients

16 natural persons – 14 persons with name and address, while 2 persons with name only –

is included in the Decision; which also records the Applicant's established location. THE

In a decision

natural persons are the victims of criminal proceedings, as well as

Applicant. After receiving the Decision, the applicant's representative hired the

contact with the presenter of the case and asked for the Decision to be amended, since in his opinion it is

Infotv does not comply. and regulations concerning the applicant - 39/2019. (XI. 19.) ORFK

instructions - its provisions. On June 12, 2020, the Applicant is represented by Infotv. § 17

requested information from the Applicant regarding whether the Applicant is a resident

for what purpose and legal basis was the transmission of its location to the recipients; also a

whether it was forwarded to other persons in addition to the recipient circle, or whether you requested information,

whether a data protection incident occurred in connection with this personal data, and whether

What stakeholder rights does the applicant have? He requested that information in his reply

stated that in the Decision, XC. of 2017 on the criminal procedure. law (hereinafter:

Be.) The Applicant's personal data were recorded on the basis of point d) of § 363, paragraph (1), so

the address of your place of residence; also the Be. Based on § 364, paragraph (1), it was delivered to the

to recipients; and the information also touched on the fact that the Be. Based on § 99, paragraph (1).

As a suspect, the applicant may not request that his data be processed in private. Applicant

in this regard, his representative referred to the fact that it had not yet taken place at that time

To report suspicions against an applicant.

According to the applicant's representative, the applicant did not provide a complete answer, thus

did not ensure the Applicant's right of access; also Requested the Decision as such

communicated to recipients who are not directly affected by it; as well as – the necessity and

in violation of the expediency requirement - personal data in the Decision, such as a

he also recorded the addresses of recipients.

According to the applicant's representative, the applicant a

with the above procedure

was violated by Infotv. the basic principles set out in § 4 - especially the goal-boundness

its basic principle - and its procedure was contrary to the Data Protection Regulations No. 39/2019. (XI.

19.) with point 30 of the ORFK instruction (requirement of purposefulness and legality).

The applicant's representative emphasized that the communication of the applicant's place of residence a

incident,

furthermore, to other persons in the recipient circle

In a decision, it goes beyond the necessity and expediency of identification, thus defeating the purpose

principle of constraint.

Based on the above, the applicant's representative requested that the Authority conduct a data protection investigation

official procedure in view of whether the Applicant has ensured the Respondent at a sufficient level

Infotv. your right of access under; also in terms of whether the Decision was violated by it

data protection provisions, whether the rights of the participants in the procedure have been violated; he also asked her

assessment of whether it was legally forwarded by the Applicant to the recipients

your location.

The applicant's representative attached to the submission the letter dated June 12, 2020 and

Your letter requesting information addressed to the respondent, in which Infotv. on the basis of § 17

is interested in what purpose and legal basis the Applicant disclosed the Applicant's "residential address" a

with recipient circle; furthermore, whether data was forwarded to persons other than the recipient circle

also for; as well as whether a data protection incident occurred in connection with this personal data.

The applicant's representative also attached to his application the Applicant June 25, 2020.

his answer dated the day of, the contents of which have been explained above. This answer is in addition to

makes general statements, contains absolutely no reference to whether it happened

data protection

too

whether the Decision was delivered. As the legal basis for the communication of the Decision, Be. Section 364 (1)

paragraph was marked by the Respondent; while with regard to the legal basis of data management -

by mistake due to an obvious typo - the Be. Section 363, subsection (1), point d) was marked, the Be.

instead of point d) of paragraph (2) of § 363. He also referred to Be. to paragraph (1) of § 99, with

that the defendant cannot request that his data be handled in private.

The Authority called the Applicant with an order to attach the documents specifically submitted to the Authority

power of attorney for proceedings; and submit a remedy for the infringement

a definite request for a decision.

The applicant's representative attached the power of attorney to his answer; also determined

also submitted a request, so that the Authority establishes the personal data

the fact of its illegal processing, and also prohibit the illegal processing of personal data,

and, if necessary, order the information of those concerned and decide the fine

about the justification of its imposition, and finally makes its decision public.

The Authority subsequently requested a statement in order to clarify the facts

called him.

According to the Respondent's answer, it is a crime of fraud committed in a business-like manner, causing significant damage

are conducting criminal proceedings against the Applicant. Necessary during criminal proceedings

became the interrogation of the applicant as a suspect, however, since he was in an unknown place and

measures taken to establish his whereabouts did not lead to results, thus

the criminal proceedings on May 1, 2020

suspended arrest warrant at the same time

in addition to its issuance, which decision was delivered to the Applicant's address in Hungary. E

following the delivery of the decision, the Applicant's representative proposed to the Respondent that

revocation of the ordered arrest warrant on the grounds that his client lives abroad and

indicated his place of residence and also attached the Applicant's proof of address. For all this

in view of the fact that the Respondent revoked the arrest warrant issued against the Applicant

and was interrogated as a suspect on July 14, 2020. According to the respondent's point of view, a

to victims during criminal proceedings

to be aware that the

a person suspected of committing a crime has been arrested or is staying

location has been established. However, the Respondent also informed the Authority that a

Due to an administrative error, the decision was not delivered to the victims,

only the suspect's lawyer, the Applicant's representative, received it. Recorded by the applicant

within their rights

by

treatment

personal details of witnesses are closed

sent documents to the Authority. The

also that the Applicant's data - according to the rules of criminal procedure - will be closed

you cannot request treatment.

By order, the Authority invited the Applicant to make another statement to clarify the facts

in the framework of

In his answer, the respondent submitted - in addition to the previous ones - that he brought it during the criminal proceedings

during the delivery of decisions, the addresses of the addressees are indicated, if a

the addressee did not request that his data be handled in private during his witness examination. In the procedure

with the exception of two victims/witnesses, the victims/witnesses did not request that their data be handled in private.

In his response, the Respondent stated that the victims were known to the Applicant

personal data, since he learned about them during the commission of the crime.

The respondent informed the Authority that he had received a copy of the entire investigation file

Applicant's representative. The applicant sent the record of the knowledge of the case file

in addition to the first pages of the witness interview minutes and wrote to the Applicant's representative, 2020.

a copy of his answer dated June 25.

The Authority called the Petitioner with an order to be sent by all the questioned witnesses

in the case of

related

a copy of your response to warnings.

He asked for his answer

from documents

it can be established that although the witness interviewed on April 1, 2019 requested his personal data -

including his name - handling it in private, however, his name is in the witness interview report

and his signature is also included.

The Authority then invited customers to comment on whether

whether they are requesting document information or whether they wish to exercise their right to make a statement.

The applicant's representative submitted observations to the Authority in the present procedure

in connection with the statements made. The applicant's representative recorded that Applicant

previously - in its information dated June 25, 2020 - it did not indicate that the recipients

they would not have received the Decision due to an administrative error. He explained that his position

according to the victims are not directly affected by the unavailability of the suspect and

the address of your place of residence; The Respondent's procedure is illegal because the Applicant and the

releasing the location of other recipients is contrary to the purpose of data transmission and the Be.

It is not absolutely necessary to achieve the purpose of communication according to § 364.

The applicant's representative submitted that the applicant makes a contrary statement in his application,

since he previously described his procedure as legal, however, he later referred to

that the delivery did not take place due to an administrative error. He further explained

that the Applicant's location was not publicly available, outside of his family

nobody knew him. The applicant was also visited personally at his place of residence abroad

unknown persons, which proves that the data of the Applicant's place of residence

removed from the Applicant's database. The applicant's residential address has been previously published by the applicant,

which it is about

knowledge. To the applicant's representative

according to the Applicant's point of view, the purposes of data management in relation to personal data

in an incompatible manner

transmits personal data to third parties

persons in a way that cannot be justified in connection with the procedure. Applicant

his representative proposed that the Authority summon the Applicant to prove his claim,

that the Decision was not sent to the recipients due to an administrative error.

The Authority

it proves it

administrative error, as well as state on what you base your claim that

The participants of the procedure could learn about the applicant's address in a different way than the Decision.

obtained in the framework of a document review

called the Applicant that

with a clarifying order

regularly

fact

4

The respondent sent the Decision's forwarding data to the Authority after printing it out

from an electronic system, according to which it is only provided by the customer gatekeeper of the Applicant's representative

delivered to your address. The respondent submitted that he was one of the victims who

private investigator, conducted research in order to establish the Applicant's place of residence,

during which he found out that the Applicant had gone abroad - South America to be exact

indicating the country as well - and he also learned his domestic address. The applicant submitted that a

victims were out of the suspect's circle of friends and acquaintances, the suspect was charged with

they were in contact with each other at the time of the act and afterwards.

In order to resolve the contradictions, the Authority - within the framework of clarifying the facts -

asked additional questions to the Respondent, since he was in a European country in the Decision

Applicant has fixed place of residence. In his response, the respondent submitted that the

occupation

victim performing activity a

after his interrogation, he informed the case investigator that the Applicant specifically

you can stay in an American country. According to the information provided by the respondent, the criminal procedure - a

at the time of the answer - it was still in the investigation phase, the investigation documents in electronic form

and it was sent by the Respondent exclusively to the Applicant's representative providing protection for the defendants.

In the case of a witness/victim, the presenter of the case failed to provide personal data in private

treatment

the name of the witness was included in the interrogation

in minutes. After the omission was discovered, the name of the witness was blacked out.

be fully implemented, since a

effectively his private investigators

considering

II. Applicable legal provisions

Infotv. According to Section 2 (3), personal data is used for law enforcement, national security and

this law shall be applied to its treatment for national defense purposes.

Infotv. According to § 3, point 2, personal data is any information concerning the data subject.

Infotv. According to Section 3.4, criminal personal data during or during criminal proceedings

prior to the crime or in connection with the criminal proceedings, the criminal proceedings

at bodies authorized to conduct and detect crimes, and a

originated at a penal institution and can be linked to the person concerned, as well as a

personal data on criminal record.

Infotv. Pursuant to § 3, point 9, a data controller is a natural or legal person, or

unincorporated organization who or which - in law you are

Within the framework defined in the mandatory legal act of the European Union - you are independent

together with others, determines the purpose of data management, for data management (including

used tool) makes and implements relevant decisions, or is

performed with a data processor.

Infotv. Pursuant to Section 3, point 10, data management is regardless of the procedure used

any operation performed on data or the totality of operations, including collection in particular,

recording, recording, organizing, storing, changing, using, querying,

transmission, disclosure, coordination or connection, blocking,

deletion and destruction, as well as prevention of further use of the data,

taking photographs, audio or video recordings, and is suitable for identifying the person

recording of physical characteristics (e.g. fingerprint or palm print, DNA sample, iris image).

Infotv. 3. § 10a. data processing for law enforcement purposes in accordance with point

threatening public order or public security in the scope of its specified duties and powers

to prevent or eliminate dangers, crime prevention, crime detection, a

to conduct criminal proceedings or to participate in these proceedings, violations of regulations

prevention and detection, as well as the conduct of the infringement procedure or on this

also in the criminal procedure or violation

to participate in the procedure,

engaged in activities aimed at implementing the legal consequences established in the procedure

organization or person (organization conducting law enforcement data management) within the scope of this activity

between and for the purpose of - including personal data related to this activity

its handling for archival, scientific, statistical or historical purposes - (law enforcement

purpose) data management.

Infotv. According to point 11 of § 3, data transmission is to a specified third party

making it available to

Infotv. According to Section 3.26, a data protection incident is a violation of data security that

personal data transmitted, stored or otherwise processed is accidental or unlawful

destruction, loss, modification, unauthorized transmission or disclosure

or unauthorized access to them.

Infotv. According to § 4, paragraph (1), personal data is only clearly defined,

it can be processed for legitimate purposes, for the exercise of rights and the fulfillment of obligations. The

at all stages of data management, the data must meet the purpose of the data management

its collection and handling must be fair and lawful. By the same token

pursuant to section (2) only personal data that is

essential for the realization of the purpose of data management, suitable for achieving the purpose. THE

personal data can only be processed to the extent and for the time necessary to achieve the purpose.

Infotv. Pursuant to § 4, paragraph (4a), you are technically competent during data management

organizational - thus especially with unauthorized or illegal processing of data, accidental

creating protection against its loss, destruction or damage -

adequate security of personal data must be ensured by applying measures.

Infotv. According to § 5 (1), personal data can be processed if

a) it by law or - based on the authorization of the law, within the scope specified therein,

in the case of data not classified as special data or criminal personal data - local

decree of the municipality orders for a purpose based on public interest,

b) in the absence of those specified in point a), those specified in the Data Management Act

it is absolutely necessary and personal data is concerned

to perform its duties

expressly contributed to its treatment,

c) in the absence of those specified in point a), the person concerned or another person

to protect its vital interests, as well as the life, physical integrity or property of persons

necessary to prevent or prevent imminent danger and thereby

you are cute

d) in the absence of what is specified in point a), the personal data is expressly provided by the data subject

made public and it is necessary for the realization of the purpose of data management and with it

cute.

(2) Special data

a) as specified in points c)-d) of paragraph (1), or

b) it can be handled if it is for the implementation of an international treaty promulgated by law

absolutely necessary and proportionate, or a fundamental right provided for in the Basic Law

enforcement, as well as national security, crime prevention and detection

or ordered by law in order to prosecute or in the interest of national defense.

Infotv. According to Section 5 (7), in the case of handling criminal personal data – if

otherwise, no law, international treaty or binding legal act of the European Union

provides - rules on the conditions for handling special data are required

apply.

Infotv. According to § 14, the data subject is entitled to have the data controller and its

personal data managed by a data processor acting on its behalf or at its disposal

in relation to the data management according to the conditions set out in this law

receive information about related facts before data processing begins

(right to prior information); upon request, your personal data and their management

related information should be made available by the data controller (for access

law); upon request, as well as personal in the additional cases specified in this chapter

have your data corrected or supplemented by the data controller (right to correction); upon request,

as well as the processing of personal data in the additional cases specified in this chapter

limited by the data controller (the right to limit data processing); upon request, as well as e

in other cases specified in chapter, the data controller shall delete your personal data

(right to erasure).

Infotv. Enforcement of the right to access pursuant to Section 17 (1).

in order to, upon request, the data controller informs the data subject that his personal data

the data controller himself, or the data processor acting on his behalf or at his direction

does it handle. Paragraph (2) of the same section states that if the data subject's personal data is

managed by a data controller or a data processor acting on its behalf or at its direction, that is

the data controller makes it available to the data subject in addition to those specified in paragraph (1).

managed by the data subject and by the data processor acting on his behalf or on his instructions

your personal data and communicates it to him

a) the source of the processed personal data,

b) the purpose and legal basis of data management,

c) scope of personal data handled,

d) in the case of transmission of processed personal data, to the recipients of the data transmission -

including third-country recipients and international organizations,

e) preservation of processed personal data

duration, on this

period

aspects of its definition,

f) the rights to which the data subject is entitled on the basis of this law, as well as the method of enforcing them

description,

g) in case of profiling, its fact and

h) data protection arising in connection with the processing of the data subject's personal data

the circumstances of incidents, their effects and the measures taken to deal with them

measures.

Infotv. 25/A. Paragraph (1) of § states that the data controller is responsible for the legality of data processing

in order to ensure all the circumstances of the data management, including especially its purpose,

as well as threats to the enforcement of the basic rights of the data subjects due to data management

enforcement of law

blocking of illegally processed personal data,

Infotv. Based on § 60 (1), it is for the protection of personal data

takes technical and organizational measures adapted to risks, including justified ones

the use of pseudonyms. These measures are taken by the controller regularly

review and amend accordingly if necessary.

Infotv. 25/K. According to § (1), if the data protection incident is likely to be

some fundamental right of the person concerned

significantly influential

may have consequences (hereinafter: high-risk data protection incident), a

with the exception of data processing for national security purposes, the data controller shall protect the data subject

informs you immediately about the incident.

The

law

in order to enforce it, the Authority, at the request of the person concerned, data protection

initiates official proceedings and can initiate official data protection proceedings ex officio.

Infotv. Based on paragraph (1) of § 60/A. in the official data protection procedure, the administrative

deadline one hundred and fifty days.

CL of 2016 on the general administrative procedure. Act (hereinafter: Act)

On the basis of §§ 7 and 8, the data protection authority procedure is referred to in the Ákr. provisions in Infotv

must be applied with specified deviations.

Infotv. According to § 61 (1) point b), it was made in the official data protection procedure

in its decision, the Authority issued Infotv. data management defined in paragraph (3) of § 2

in connection with operations, it may be determined that personal data is being processed illegally

fact, you can order the correction of personal data that does not correspond to reality, you can order it

the

deletion or destruction,

may prohibit unlawful processing of personal data, may prohibit personal data

forwarding or handing it over abroad, you can order to inform the person concerned, if so

data controller unlawfully refused, and may impose a fine.

Infotv. According to paragraph (2) of § 61, the Authority may order in its decision - the data controller,

and by publishing the identification data of the data processor - to the public

making it, if the decision affects a wide range of persons, by a body performing a public task

brought in connection with his activity, or what happened

gravity of infringement a

justifies disclosure.

Infotv. According to § 61, paragraph (4), point a), the amount of the fine is from one hundred thousand to twenty million

can range up to HUF. Infotv. Based on paragraph (5) of § 61, the Authority in deciding whether

is the imposition of a fine according to subsection (1) point b) bg) justified, or the fine

when determining its rate, it takes into account all the circumstances of the case, thus

in particular, the size of the circle of those affected by the infringement, the gravity of the infringement, the behavior

culpability, as well as whether the offender was previously convicted of

violation of the law related to the management of personal data.

Infotv. Pursuant to § 71, paragraph (1), during the Authority's proceedings - that

to the extent and for the time necessary to conduct it - you can manage all personal data,

as well as classified as a secret protected by law and a secret bound to the exercise of a profession

data that are related to the procedure and that are managed by the procedure

necessary in order to conduct it successfully. According to paragraph (2), the Authority is

documents, data or other means of proof legally obtained during its procedures by others

you can use it in your procedure.

The Be. According to Section 99 (1), the court, the prosecution and the investigative authority

orders on motion that the injured party, the pecuniary interest and other interested parties are these

the name, birth name, place of birth and

time, mother's name,

residential address, notification address,

your citizenship, identity document number,

your actual location, delivery address, and electronic contact information

be treated.

The Be. According to § 99, paragraph (5), personal data managed in private is only handled by the person acting in the case may be handled by the court, prosecutor's office and investigative authority, and they are subject to the consent of the data subject

only without

a) to the court, prosecutor's office and investigative authority handling the case,

b) performing tasks related to victim assistance for the victim assistance service,

and to the probation service for the purpose of conducting the mediation procedure, e

can be transmitted to the extent absolutely necessary for the performance of tasks.

The Be. Pursuant to Section 99 (6), the court, the prosecutor's office and the investigative authority

ensures that the personal data managed in private does not become part of the other data of the procedure

become known.

The Be. According to § 100, paragraph (1), the case files of the procedure

a) the accused and his defense counsel after questioning the accused as a suspect,

b) the victim in connection with the crime affecting him and

c) the other interested party and the property interested party in the circle affecting him

you can get to know it on a motion to this effect.

Paragraph (2) of the same section provides that according to paragraph (1).

the right of access extends to all case files of the procedure, including the court and the prosecutor's office

and obtained by the investigative authority or by persons participating in criminal proceedings

submitted and attached documents and additional means of proof.

The Be. According to § 100, paragraph (3), the prosecution does not form part of the case files of the procedure

and the investigative authority in connection with the exercise of supervision and control

generated case file, especially the prosecutor's order, investigation plan, draft decision and

the presentation.

Pursuant to paragraph (4) of the same section, the court, the prosecutor's office and the investigator

authority to get to know the case files of the procedure

a) by enabling the inspection,

b) in the case of a separate motion or consent to this effect, about the content of the case file

providing clarification, providing information,

c) by enabling the making of a copy or recording for one's own part,

d) the case file and the court, the prosecutor's office and the investigative authority about the case file

by delivering a prepared extract or copy, or

e) in other ways defined by law

9

ensure.

The Be. Paragraph (5) of Section 100 stipulates that the right to access is not affected by the proceedings in private

special provisions regarding the managed case files, as well as the confidential handling of the data

obligation.

The Be. According to § 100, paragraph (6a), if the procedure is ongoing due to several acts, and there are such

an act for which suspicion has not yet been reported, the court, the prosecutor's office

and the investigating authority for this act is the suspect and his defense counsel

with respect to the right of access, or any access listed in paragraph (4).

method without indicating the case files - in the absence of a different provision of this law -

can limit, on which it makes a decision.

The Be. Paragraph (1) of § 102 provides that the court, the prosecutor's office, and the

the investigating authority handles the e

in law

specific case file. Pursuant to paragraph (2), the closed file is the

and in the absence of a different order of the trial court or prosecution, only the court, that is

the public prosecutor's office or the investigative authority can find out.

According to paragraph (3) of the same section, in case of closed handling of the case file, the court,

prosecutor's office and the investigative authority

a) ensures that the closed file and its contents are different from the procedure

do not become known from your case files and data,

b) ensures the knowledge of the case files in such a way that it does not result in closed doors

getting to know the handled case file.

The Be. According to paragraph (1) of § 363, the decision shall be divided into the introductory part, the operative part,

it is divided into a justification and a closing part. Pursuant to paragraph (2) d) of the same section

the introductory part

includes the data necessary for identification

designation to whom the provision applies. According to paragraph (4), the justification is

significant facts established by the prosecutor's office or the investigative authority, the decision

the underlying legislation and, if necessary, their interpretation, as well as these

contains an explanation of the substantive provision in context.

The Be. Based on § 364, paragraph (1), if this law does not provide otherwise, the decision

it must be communicated to those who are directly affected by a provision of the decision.

The Akr. Pursuant to § 51, paragraph (1), if the authority does not take action within the time limit, § 43 (1)

of those specified in paragraphs a) and b), the administrative deadline is exceeded, or

automatic decision-making, or unreasonably disregards the rules of the summary procedure, that is

as a fee to be paid for conducting a procedure or according to the Act on Fees

for administrative official procedures or for the use of administrative services

an amount corresponding to the paid administrative service fee, or in the absence of this, ten thousand forints

pays the requesting client, who is also exempt from paying the procedural costs.

The decision is also referred to in Art. Sections 80 and 81 shall apply.

III. Decision

III.1. Validation of the applicant's right of access

The Authority found that the Respondent violated the Applicant's right to access

right by considering the submission dated June 12, 2020, to June 25, 2020.

did not answer all of the Applicant's questions in the transcript dated

in the framework of The respondent's response did not include whether a data protection incident had occurred

Regarding the Applicant's personal data, he did not declare that the Applicant

to whom you forwarded your personal data, and also to a non-existent legal place - Be. Section 363 (1)

paragraph point d) - referred to as the legal place on which the Decision is based

content.

III.2. Inclusion of recipients' personal data in the Decision and in private

failure to manage data

In addition to the above, the Decision contains the names of the recipients, such as the Applicant and the injured parties, and -

with the exception of two recipients - their delivery address. The recipients - not including the Applicant

his name - the inclusion of his name and delivery address in the decision defeats the purpose

the principle of bound data management, since their inclusion is completely unnecessary, it

it can only be for an administrative reason. In general, the Authority records that the recipients

including your delivery details – name and address – on a separate delivery clause as

data security measure would meet the requirement of data minimization.

During the procedure, the Authority noticed ex officio that the Respondent's name was also violated

stated in the Decision, who during his witness examination on April 1, 2019

proposed that all his personal data, including his name, be handled in private.

Furthermore, it can be established that the interrogation protocol is also in the investigative documents

includes your name and signature as your personal data. With all this, the witness requested

personal data not at the disposal of the data subject and the Be. applicable data protection regulations

treated according to; thus violated - discussed in detail among the applicable laws - a

On. the provisions of § 99, § 100 and § 102. The investigator is involved in this

authority's information that "the Be. Based on Section 99 (1), the court, the

the prosecutor's office and the investigative authority order on motion that the victim, the interested party and

the name, birth name, place and time of birth of the other interested party or their assistant,

mother's name, nationality, identity document number, address, notification

address, actual location, delivery address, and electronic contact information

should be handled in private" declared that "I understood the warning, my personal data

please handle it closed". From all of this, it can be established that the Applicant is one of them

in the case of the affected victim, he ignored the motion regarding closed data management. THE

At the same time, the authority took into account that from the interrogation protocol and the Decision

only the name and, in the case of the former, the signature of the Applicant and Applicant could be known

before his representative. The name of the affected victim is Applicant - the crime charged to him

due to its nature and circumstances - he necessarily knew it. From the investigative files

it appears that the Applicant and the victim know each other personally and have met before

during which they entered into a written civil contract with each other.

The respondent - in response to the Authority's question in this regard - stated that the procedure was different

actors did not know each other's or the victims' data recorded in the Decision,

only the representative of the Applicant got to know the documents of the investigation.

Based on the above, it can be established that a data protection incident has occurred, which at the same time - a

due to the circumstances explained above - is not considered high risk.

11

for transmission, which the victims,

In the future, the Authority wishes to emphatically emphasize that although the above-mentioned a

They can be established in relation to the decision, but at the same time it is necessary to point out that on

except in the case of the person concerned, who has requested that all his personal data be handled in private,

no such data was found

or Applicant no

they could have known me in the framework of the criminal proceedings. Applicant as burdened residential and

the details of your location are necessarily included in the investigative file; on the one hand, this is true

mandatory data to be recorded as part of the suspect's interrogation report

in the case of, on the other hand, submissions received during the investigation and made part of the investigation file,

and also in the case of official records and decisions of the investigating authority. So that's it

data to the victims in accordance with the rules of criminal procedure in the context of document recognition - the Be.

According to the provisions of § 100 - they can get to know. The same is true in the reverse case, that is

The Applicant and the Applicant's representative are also entitled - following the questioning of the suspect

was to get to know the data of the victims/witnesses who did not request that their data be kept private

treatment, as the suspect and his defense are also entitled to this right.

of the Authority's request

partially approved and established by the

violation of the principle of data saving and purpose-boundness, since in the Decision

The applicant has included his delivery address unnecessarily. Furthermore, the Authority ex officio

found that the Decision unnecessarily contained the names of the victims and delivery

address.

Based on the above, the Authority is Infotv. ex officio according to § 61, subsection (1) ba).

also established that the Respondent handled the personal data illegally -

violating data security requirements - a

witness to his confidentially managed data

By including it in the decision and by not providing the interrogation

closed handling of the data of the affected victim/witness in the protocol. With all this data protection

caused an incident.

III.3. Transmission of data regarding the applicant's location to recipients

The Authority accepted it, given that there is no evidence to the contrary

He requested his statement supported by the document that the Resolution

it was not delivered to any person other than the Applicant's representative.

At the same time, the Authority found that he Requested the Decision - his original intention

according to - he wanted to deliver it to the recipients indicated on it without legal basis. Obviously
The Respondent's argument that the Decision applies to recipients other than the defendant is incorrect
also contains a direct provision. There is no doubt that the victims have the right to
to be informed about the progress of criminal proceedings, however, in this regard, the suspended investigation continues
the delivery of a decision on its continuation to them is justified. All this - and
only this - the Be. Paragraph (2) of § 397 also prescribes it as a separate communication obligation. E
the Be is required locally. description of the relevant part of the commentary: "The decision
as a general rule, it must be communicated to those who are directly affected by any of its provisions. The direct
involvement must stand out from the introductory part, the decision itself contains that
to whom its provisions apply, such as, for example, regarding the advance payment of the assigned counsel's fee
decision extending the deadline of the ongoing investigation against the defender
a decision refers to the suspect, a decision rejecting a motion refers to the petitioner
is directly affected, while the decision ordering merger, separation or transfer
it does not affect a person directly involved in criminal proceedings. The communication obligation
exceptions to the main rule can be divided into two groups, in one case the decision cannot be made
to communicate to the data subject even if one of its provisions directly applies to him, so a
On. In view of § 250, a permit for the use of a concealed device is excluded
communication to the person concerned in the permit. In the other case, the decision
it must also be communicated to those who are not directly affected by it, which may be based on a general nature
available, for example the Be. Pursuant to § 42, paragraph (3), the decision communicated to the accused is a

with defender, the Be. Pursuant to § 72, paragraph (2), the decision communicated to the defense counsel is legal
representative must also be notified, but the Be. communication obligation for certain decisions
also stipulates related to it, so the Be. Paragraph (2) of § 350 is the transfer, the Be. § 381, paragraph (2).
rejection of the complaint, the Be. Paragraphs (2)-(3) of § 397 suspend the proceedings and Be.
§ 401 provides that in case of termination of the procedure, it is decisive in the given issue

to whom the decision must be communicated."

According to the Authority's point of view, recording the Applicant's place of residence abroad a

In a decision - the Be. Subject to § 393, paragraph (4) - justified. That investigative authority

is considered a significant fact established by

arrest warrant and could make arrangements to continue the investigation.

In the opinion of the Authority, the fact that

Suspicion against the applicant - obviously he belongs to the unknown place

due to his stay - was not disclosed when the Decision was made. Although the then effective Be. –

contrary to the law currently in force - the crime did not yet contain it

a person suspected of having committed it as a person participating in criminal proceedings, however

- as can be seen from the justification of the current law - the introduction of this role is earlier

adapted to legal practice.

In this regard, the Authority rejected the request.

ARC. Legal consequences

The Authority is Infotv. Ordered by the Applicant Respondent based on Section 61 (1) point bf).

supplementing your information by whether a data protection incident has occurred or whether

to whom the Decision was communicated.

The Authority is Infotv. On the basis of § 61 (1) point (ba), it states that the Respondent

was violated by Infotv. Paragraphs (1)-(2) and (4a) of § 4 by stating that in the absence of a legitimate purpose,

unnecessarily recorded the names of the natural persons involved as victims and

delivery address and the Applicant's delivery address in the Decision.

Also Infotv. Pursuant to Section 61 (1) point ba), the Authority ex officio

establishes that the Applicant complies with the relevant safety regulations during its procedure

violated Infotv by failing to implement it. 25/I. because no

ensured the security of the witness's confidential personal data.

In considering the imposition of the fine, the Authority assessed the fact that a

after the discovery of the error, the Respondent executed the blackout of the witness's name out of line
in documents. By definition, in the case of the Applicant - who has already become aware of the personal data -
cannot handle the results of this measure. However, the Authority is the legal consequences
in its consideration, it also took into account the fact that the Respondent ultimately did not send out the Decision
- In addition to the applicant's representative - to recipients; furthermore, although unnecessarily, the Decision
it contained personal data - with the exception of one person - that is investigative
from documents
available
from the documents, that the Applicant was this person during the commission of the act he was charged with
he also necessarily got to know his name. Furthermore, all the circumstances of the case are taken into account
taking into account, in particular, the size of the circle of those affected by the infringement, the gravity of the infringement, as
well as
whether the personal data was previously established against the offender
violation of the law related to the handling, the Authority decided not to impose a fine
justified.
are legally identifiable. The
can also be established a
13
The Authority is Infotv. Based on § 61, paragraph (2), point b) of the decision, the Customer
also ordered the disclosure of his identification data, as it is a public duty
brought in connection with the activities of a provider. During the procedure, the Applicant is a
in his answer, he made the statement that the decisions made during criminal proceedings a
addresses of recipients are indicated. This confirms that it is common practice to
editing decisions in this way, if without purpose or legal basis in a general manner
the names and addresses of the recipients are indicated on the decisions, it may mean a systemic error.
During the procedure, the Authority exceeded Infotv. One hundred and fifty days according to paragraph (1) of § 60/A

administrative deadline, therefore the Ákr. On the basis of point b) of § 51, he shall pay HUF ten thousand to the Applicant.

A. Other questions

Infotv. According to § 38, paragraph (2), the Authority is responsible for the protection of personal data,

and the right to access data of public interest and public interest

control and promotion of the validity of personal data in the European Union

facilitating its free flow within.

The Authority's jurisdiction covers the entire territory of the country.

The Akr. Based on §§ 112 and § 116 (1), as well as § 114 (1), the

a decision can be appealed through an administrative lawsuit.

* * *

The rules of the administrative proceedings are set out in Act I of 2017 on the Administrative Procedures

(hereinafter: Kp.) is determined. With the decision of the Authority based on Section 12.(1) of the Administrative Code

the administrative lawsuit against falls within the jurisdiction of the court, the lawsuit is referred to in the Kp. Section 13 (3)

Based on subparagraph a) point aa), the Metropolitan Court is exclusively competent. THE

CXXX of 2016 on civil procedure. to the law (hereinafter: Pp.) - the Kp. § 26

(1) applies - Kp. Based on point b) of paragraph (1) of § 27 a

legal representation is mandatory in a lawsuit within the jurisdiction of a court. The Kp. Section 39 (6)

according to paragraph - if the law does not provide otherwise - the submission of the statement of claim a

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

The Kp. Paragraph (1) of § 29 and, in view of this, Pp. It is applicable according to § 604, that is

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).

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

The place and time of submitting the claim is set by Kp. Section 39 (1) defines it. THE

information on the possibility of a request to hold a hearing in Kp. Section 77 (1) and (2)

based on paragraph The amount of the administrative lawsuit fee is determined by the 1990 Law on Fees

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

from the payment of the Itv. Paragraph (1) of § 59 and the Itv. Based on point h) of paragraph (1) of § 62

exempts the party initiating the procedure.

If the Customer does not adequately certify the fulfillment of its obligations, the Authority shall

considers that the obligation has not been fulfilled within the deadline. The Akr. According to § 132, if

client in the Authority's final decision

did enough, that is

can be executed. The Authority's decision in Art. according to § 82, paragraph (1) with the communication

becomes permanent. The Akr. Pursuant to § 133, enforcement - if it is a law, or

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

not as an obligation

president

Dr. Attila Péterfalvi

c. professor

pursuant to § the execution - if it is a law, government decree or municipal authority

the local government decree does not provide otherwise - the state tax authority

undertakes. Infotv. Based on § 61, paragraph (7), the implementation of the Authority's decision is carried out by a

to carry out a specific act, specific behavior included in a decision,

in relation to the obligation to tolerate or stop, the Authority undertakes.

Budapest, according to the electronic signature