Case number: NAIH-3748-1 / 2021.

(NAIH / 2020/5483.)

Subject: Infringement decision

DECISION

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

(registered office of […]; hereinafter referred to as the “Customer”)

data management related to the electronic monitoring system - the purpose of the data processing,

the principle of data protection and appropriate prior information

the processing of personal data by natural persons

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

Regulation (EU) No 2016/679 of the European Parliament and of the Council of

ex officio in a data protection official procedure

1. Notes that the Customer has infringed Article 5 (1) of the General Data Protection Regulation

the principle of purposeful data processing under paragraph 1 (b) on the grounds that it is unlawful

operated cameras 9, 10, 11 and 23 during the period under review;

2. Finds that Customer has violated Article 5 (1) of the General Data Protection Regulation

the principle of data protection under paragraph 5 (c) by operating in accordance with

15, 18, and 21, and operates cameras 3, 13, 14, 16, 17, 19, 20, and

No. 22 cameras that they were unsuitable or unsuitable for the Customer

to achieve the data processing purpose set by the

3. Notes that the Customer has infringed Article 5 (2) of the General Data Protection Regulation

the principle of accountability under paragraphs 22 and 23.

change the angle of view of the number of cameras;

4. Finds that Customer has violated Article 5 (1) of the General Data Protection Regulation

the principle of lawful and fair processing in accordance with paragraph 1 (a)

operating camera 23 in the head of the institution's office;

5. finds that the Customer has infringed Article 6 of the General Data Protection Regulation

by processing the personal data of data subjects on an inappropriate legal basis

in the context of camera surveillance;

6. Notes that the Customer has breached Article 5 (1) of the General Data Protection Regulation

the principle of transparency under paragraph 13 (a) and Article 13 of the General Data Protection Regulation.

Article 2 (1) to (2) of the Directive, since it did not provide adequate and transparent information

data management related to camera surveillance;

7. Instructs the Client that, with the exception of Cameras 5, 15, 18 and 21,

in view of the fact that they have already been decommissioned by the Customer, terminate the

unlawful data processing in violation of the purposeful data processing No. 9, 10, 11 and 23

for cameras, by deactivating the cameras or their viewing angle

by modifying it so that the data processing complies with lawful data processing

requirements;

8. instructs the Client to operate on an appropriate legal basis by the Authority

cameras that are not used for lawful purposes and are fit for purpose; and

provide adequate and transparent information on them.

....

....

1055 Budapest

Falk Miksa utca 9-11

Tel .: +36 1 391-1400

Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu

www.naih.hu

The Authority also

500,000, ie five hundred thousand forints

data protection fine

the Client is obliged to pay.

***

Taking the action provided for in clauses 7 and 8 from the notification of this decision to the Client

within 30 days of receipt of the supporting evidence

together - to the Authority.

The Authority shall impose a data protection fine within 15 days of the decision becoming final

centralized collection account for centralized revenue collection (10032000-0104042500000000 Centralized collection account

IBAN: HU83 1003 2000 0104 0425 0000 0000)

to be paid for. When transferring the amount, NAIH / 2020/5483. JUDGE. should be

to refer to.

If the Customer fails to comply with its obligation to pay a data protection fine within the time limit, a

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

interest that is valid on the first day of the calendar half-year affected by the delay

equal to the basic interest rate.

Failure to comply with data protection fines and late payment and obligations

In that case, the Authority shall start implementing the decision.

There is no administrative remedy against this decision, but from the date of notification

within 30 days of the application lodged with the Metropolitan Court

can be challenged in a lawsuit. The enhanced defense does not affect the time limit for bringing an action. THE

the application must be submitted to the Authority, electronically, together with the case file

forward it to the court. The request to hold a hearing must be indicated in the application. THE

during the period of enhanced defense, the court shall act out of court, including on appeal

procedures. For those who do not benefit from full personal exemption a

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

Legal proceedings are mandatory in proceedings before the General Court.

EXPLANATORY STATEMENT

I. Facts, antecedents

1. A notification was received by the Authority on 28 May 2018 stating that the applicant is

He objected to a customer-operated home-based camera system. According to the announcement

all rooms are equipped with cameras except washbasins, changing rooms and the head nurse

room. On the ground floor there is a living room for 1-2 people with a camera

which is covered with a piece of cardboard. According to the announcement, the cameras are for workers

they are also used to monitor their work, the recordings being made on a daily basis

they look back.

2. The Authority shall comply with Article 57 (1) (f) of the General Data Protection Regulation and

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

(hereinafter: the Information Act) on the basis of the notification pursuant to Section 38 (3) (a)

3

NAIH / 2018/3445 / V. initiated an investigation with camera surveillance under case number

in the context of related data management.

In the course of the investigation procedure, it became clear from the Client's statements that the twenty-five

a non - sound recording electronic surveillance system consisting of a camera - one of which a

was covered at the time of the investigation procedure - the Customer operates the Home and its occupants

the protection of property and the maintenance of rules of procedure and human life,

to protect physical integrity, personal liberty and trade secrets. The Customer is the data management

the legitimate interests of the employer and the consent of those concerned

marked.

According to the statement made by the Client in the investigation procedure, it has a legitimate interest on the one hand

and the cameras are needed because the yard of the Home is fenced, however

does not prevent foreigners from entering through the fence. The ground floor windows of the building a

easily accessible from ground level, easily accessed by unauthorized persons. The cameras

however, they help prevent these.

According to the statement made by the Customer in the investigation procedure, the food purchased by the residents is

different

to clarify disputed situations related to the theft of residents by

cameras in kitchenettes. According to the Customer's statement in the kitchenettes

it happens that the residents take away personal belongings and food from each other

they are suspected of theft and all this leads to their deterioration. The camera recording

however, after viewing, they will calm down and return to their original state. Besides that

it is also possible to trace when someone falls, at what angle and in what way, so it is

Your home staff can take a targeted approach to treatment. Operating in the kitchenettes

therefore, in addition to protecting property and preventing theft, cameras are urgent

in the event of an accident, they increase targeted intervention and the survival of those cared for.

In connection with the monitoring of community sites, the Client stated in the inspection

in the event of a dispute between residents, they may find out by recording that

who committed the first act, as there were also disputes between two residents, which

led to action. In addition, there has been a case of one of the nurses washing up

finished, and the inhabitant hoed so much that he beat his hand, which had to be sewn together. Because of this

a relative of the resident threatened the Client with a lawsuit because, in his opinion, the nurse

he dropped his father. However, the recording was able to clarify the case and protect them

the interests of their staff. The cameras in the public areas are therefore at home

in addition to the purpose of protecting property, as several

atrocities have taken place between residents of the community and have been

was clarified by recording cameras.

In connection with the cameras operating in the office premises, the Customer stated that a

investigation procedure that the payment to residents in addition to the protection of property

also serves to document. If the resident is not under guardianship, the Home is required to pay money

give for. On several occasions, however, the resident or a relative of the resident did not

even after signing the acknowledgment of receipt, he admitted that he had taken money and suspected it

an employee of the Home or the Home that the document was forged. The office

The purpose of the cameras in the rooms is therefore to protect the safe, office staff,

and protection of documents and equipment stored in the office. On the other hand, the office

In addition to the official documents of the Home, there are also documents related to the residents.

The basic property protection interest of the Client is also the protection of the property of the Home and the residents,

which is also assisted by cameras.

Based on the information obtained in the test procedure with the electronic monitoring system

to view the data recorded in addition to the persons authorized to do so by law a

a representative of the maintainer to detect breaches and verify the operation of the system

authorized or instructed by the employee responsible for data processing. A possible system

the contact required for error correction can be resolved by logging in to the maintainer. Entry

ID is one piece. The system does not log entries. The cameras are exclusively for

are available from the maintainer only from the central computer located in the Home office.

According to the statement made by the Customer during the investigation procedure, the recordings recorded by the cameras

it is stored for a maximum of three working days when not in use. Whose right you are right

interest in the recording of the data of the recording, three from the recording of the recording

within a working day, request proof of his right or legitimate interest that the data,

the recording must not be destroyed or deleted by its operator. So far, this is mainly

for security purposes, for example, when the elderly were wanted to be found, respectively

workers' missing personal belongings. In addition, during the quarrels and debates of the elderly

protection of physical integrity and control of the presence of unauthorized persons

recordings are also used for this purpose. However, recordings are not made on a daily basis

will be viewed only in the event of a reported problem and will not be forwarded to anyone.

According to the statement made by the Client in the investigation procedure, the employees and the residents a

prior to the installation of the camera system, they were given verbal information on how to set up the system

and its purpose and will be informed in writing after the installation is completed,

a written declaration of receipt and acknowledgment of the information

they did. These statements are available at the office. In addition, employees a

on the operation of the camera system, a workshop prior to its installation

also informed during the presentation of the data protection policy, who are the so-called

By signing the “GDPR Privacy Education Journal” and the Privacy Policy

took note of the information. The Client sent one of these documents to the Authority

confidentiality statements signed by employees, “employment contract clause is

on the knowledge, application and confidentiality of data protection rules "

document signed by the employees on June 13, 2018

protocol on data protection education.

The Authority's question of who is considered to be an electronic surveillance system

to view data for persons authorized to do so by law and what the law is

the Client has stated that the representation of […] in the NGOs

In accordance with the provisions of the law, the Board of Trustees provides and maintains contact with third parties

and exercise the employer's authority under the Labor Code

Pursuant to Act I of 2012 (hereinafter: Mt.) against employees of the Home.

According to the statement made by the Client in the investigation procedure, it also employs forty people

it is home to eighty-two residents.

The Authority in the investigation procedure has repeatedly explained that the office premises

Due to the location of the cameras, the data processing related to the operating cameras violates the

purposeful data processing pursuant to Article 5 (1) (b) of the General Data Protection Regulation

principle. Based on the camera images sent to the Authority, the angle of view of the cameras towards the employees

watching their activities throughout the day. In the Authority's view, the Home,

and the most suitable means of protecting residents' documents and money is a lockable one

wardrobe or safe.

The Authority also did not consider the operation of cameras in the kitchenette to be acceptable,

whereas, in its view, they are not fit for purpose. The Authority explained that

camera shots alone can only capture that, if any, someone

it takes some food with it, but it is not suitable to prove that it is

a person takes food held by someone else. With that statement

and that, in the event of an emergency in these rooms, the cameras increase the

targeted intervention and the survival of carers, the Authority is of the opinion that

in the case of an emergency intervention, it is unrealistic and precisely the effectiveness of the intervention

would be reduced if you tried to view camera footage before the operation

reconstruct the circumstances of the accident. The right and fast supply of the right workforce

must be provided.

With regard to the monitoring of community sites, the Authority was also of the opinion that this

no cameras are needed in the rooms either. He made a statement in connection with the disputed events

with a view to finding out, where appropriate, who first resorted to the act,

the Authority's position is that it is essential that the dispute be resolved or that it be addressed in the future

to prevent similar situations in which it is not clarified a

most importantly, who did the first act.

The case where one of the nurses washed and the resident […] and then the relative of the resident

threatened a lawsuit against the home because she believed the nurse had dropped her father and the

camera recording could clarify the case and protect the interests of their co-workers in this

the case has achieved its purpose, however, the one-off cases do not make it proportionate to one

data management. In that case, the Authority would consider it necessary in this respect to:

the protection of employees as a purpose of data processing where similar incidents often occur

cases, however, the Client did not mention several specific cases in the investigation procedure.

Where the purpose of operating the camera system in public areas is to:

protection of property, the Authority would consider it acceptable that the camera in question

angle of view - for the purpose of Article 5 (1) (b) of the General Data Protection Regulation

following the principle of data protection. The cameras are like that

However, no such transfers took place during the investigation procedure.

On the basis of the above, the Authority found in the investigation procedure that the employees

monitoring is not lawful for the purpose specified and pursued by the Customer, while

the purpose of data management for security purposes is not clear, not clear. Position of the Authority

nor was it substantiated whether data processing was necessary for this purpose at all

to achieve the interest behind it. Consequently, the Authority concluded that

Customer handles personal data with the electronic monitoring system without a legitimate purpose

in breach of Article 5 (1) (b) of the General Data Protection Regulation.

point.

The Authority further found that, as the Client merely invoked a legitimate interest

but did not weigh up the interests in bringing proceedings

personal data of employees, in breach of Article 6 of the General Data Protection Regulation

Paragraph 1 (f).

The Authority also found that the Client did not provide adequate and comprehensible information

information to employees in breach of Article 13 of the General Data Protection Regulation.

Article.

In view of the above, the Authority is required to comply with Article 58 (2) (b) and (b) of the General Data Protection

Regulation

d) and Infotv. He was called upon three times pursuant to Section 56 (1)

(Notices NAIH / 2019/5088, NAIH / 2019/5088/4 and NAIH / 2020/2767)

Customer to terminate the processing of data related to camera surveillance,

whereas it is illegal and seriously violates data protection requirements, as well as all

Customer's employees 'and residents' right to the protection of personal data. THE

Authority also drew the Customer's attention to the fact that the data processing only then

can be done if the Customer ensures its legality and the general data protection regulation

compliance with its requirements.

6

The Client responds to the Authority's need for data management in several ways and forms

justified, in addition to supporting an impact assessment as well as data protection

also drafted regulations and conducted a balance of interests. These were made in April 2020

documents, in the same way but in the same way as

Customer Statements - The need for data management has not been substantiated. By the notifier

the challenged data management was still not based on adequate requests despite the Authority's requests

and violated the privacy requirements of both the Customer

the right of both employees and residents to the protection of personal data. The client

and, although he stated that he had complied with the requirement to provide adequate information,

and a data protection policy, but these did not comply with the general rules

the rules of the Data Protection Regulation.

3. The Authority therefore Pursuant to Section 58 (2) (a), closed the investigation procedure,

and Infotv. Pursuant to Section 60 (1), ex officio NAIH / 2020/5483. case number

initiated a data protection authority procedure to investigate the data management covered by the notification, which

the purpose of the data processing, the legal basis, the principle of data saving, the appropriate preliminary

information. The examined period is from 25 May 2018 to the present

until the date of initiation of the official data protection proceedings - 16 July 2020

period, provided that the subsequent data protection proceedings,

New regulations dated 1 October 2020, documents on data management a

a data protection fine under Article 83 (2) of the General Data Protection Regulation

the determination of the amount of the decision and the execution of the decision

to be evaluated.

The Authority shall inform Infotv. In view of Section 71 (2), in the present data protection authority proceedings

use the test procedure lawfully obtained and by 16 July 2020

documents and data generated.

On the one hand, the Client has stated that it maintains its statements made during the investigation procedure

with regard to the need for data management, it cannot present new facts.

On the other hand, however, he amended his rules. The Customer in the data protection authority proceedings

and the new camera code sent on 1 October 2020,

and marked the exact location of the cameras in a balance of interest test by them

the area observed and the value to be protected as follows:

Camera 1: opposite the main entrance door; the observed area is the main entrance door and foyer; the

value to be protected protection of persons and property, protection of business secrets and private secrets.

Camera 2: nurse room above front door; the observed area is the nursing home; the value to be protected

protection of property, business secrets and privacy, protection of personal data.

Camera 3: to the left of the main entrance; the observed area is the lounge area; the value to be protected

property protection, personal protection, complaint investigation.

Camera 4: out of service; vip room, but since living room has been designed, so here the camera is already a

terminated prior to the investigation procedure.

Camera 5: ground floor kitchenette; the Authority objected, so the camera was discontinued.

Camera 6: ground floor rear corridor; the observed area is the exit facing the courtyard; to be protected

value protection of persons and property; preservation of business secrets and private secrets.

Camera 7: upstairs rear aisle; the observed area is the rear of the ground floor corridor; the

value to be protected protection of persons and property, protection of business secrets and private secrets.

Camera 8: upstairs nurse's room; the area observed is the area of the upstairs nurse's room; to be protected

value protection of property, trade secrets and privacy, protection of personal data.

7

Camera 9: dining room; the observed area is the dining room and its surroundings; the value to be protected

personal protection.

Camera 10: dining room; the observed area is the dining room and its surroundings; the value to be protected

personal protection.

11. camera: kitchen; the observed area of the kitchen room; the value to be protected is property protection.

12. camera: kitchen; the observed area is the economic entrance; the value to be protected

property protection.

Camera 13: upstairs lounge; the observed area is to the left of the upstairs lounge; to be protected

value property protection, personal protection, complaint investigation.

Camera 14: upstairs lounge; the observed area is the right side of the upstairs lounge; to be protected

value property protection, personal protection, complaint investigation.

15. camera: upstairs kitchenette; it was objected to by the Authority and was therefore terminated.

Camera 16: 2nd floor lounge; the observed area is the right side of the 2nd floor lounge; the

value to be protected property protection, personal protection, complaint investigation.

Camera 17: 2nd floor lounge; the observed area is to the left of the 2nd floor lounge; to be protected

value property protection, personal protection, complaint investigation.

Camera 18: 2nd floor kitchenette; it was objected to by the Authority and was therefore terminated.

Camera 19: 3rd floor lounge; the observed area is the right side of the 3rd floor lounge; the

value to be protected property protection, personal protection, complaint investigation.

Camera 20: 3rd floor lounge; the observed area is to the left of the 3rd floor lounge; to be protected

value property protection, personal protection, complaint investigation.

Camera 21: 3rd floor kitchenette; it was objected to by the Authority and was therefore terminated.

Camera 22: ground floor office, secretariat; the observed area is the office area; the value to be protected

protection of property, business secrets and privacy, protection of personal data.

Camera 23: ground floor office, meeting room, head of institution's office; the observed area is the office

area; the value to be protected is the protection of property, protection of payments and privacy.

24. camera: basement; above the door to the toilet opposite the lift; the observed area is

basement corridor; the value to be protected is property protection.

25. camera: basement; has been abolished.

The Camera Regulations, which entered into force on 12 June 2020, were also sent to the Authority

and according to its interest balance test dated 12 June 2020, only No. 4

the camera was taken out of service while the regulations and test were revised on 1 October 2020,

according to the current version, it was decommissioned - in addition to the camera No. 4 - in the 5th, a

Cameras 15, 18, 21 and 25. That is, the Customer, although the data protection authority procedure

but five cameras were taken out of service and in view of this change

has modified his camera policy and interest balance test.

Annex 4 to the Camera Regulations dated 15 June 2020 - which is in full

identical to Annex 4 of 1 October 2020 - contains data management

information on The prospectus is addressed to employees, residents and visitors of the Home as

affected. The brochure draws the attention of stakeholders to the operation of the camera system, respectively

informs them that by “entering the territory of the Institution and here

consent to the processing of the data relating to the imaging. "

According to this guide, “the operation of the camera system and the recording of images a

aims to protect human life, physical integrity, personal liberty in the territory of the Institution,

protection of property, protection of business, private and payment secrets, protection of work and property, a

complaint handling. Within this framework, the aim is to detect violations, to catch the perpetrator, e

prevention of offenses and as evidence in this context

be used in the context of an official procedure. "

According to this prospectus, “the operation of the camera system is partly the responsibility of the Institution

which is supported by a balancing test, and

consent-based data processing. "

According to this information, the images will be stored for a maximum of 10 business days

depending on the size of the recorded material, depending on the storage and movement.

This leaflet also states that 24 out of the 25 cameras located in the Home area

and the exact location of the cameras and the area they are observing

information on the operation of the camera surveillance system.

According to this information sheet, the data subject may also request information on the processing of his or her personal

data,

you can request that they be corrected, deleted or blocked.

The prospectus also refers to the fact that the camera regulations are available to the head of the institution

and at the office of the Data Protection Officer.

According to the statement made by the Client in the data protection official procedure, NAIH / 2020/2767.

already sent in an e-mail dated 29 April 2020

has informed the Authority that in order to comply with the Authority, the Client

has completely reviewed the previous camera regulations, conducted a balancing test and the new one

regulations and a test to the Authority. The Customer is the data protection authority

In the proceedings, he again sent this April camera regulations and the balancing test

In the latter document, it was pointed out in relation to each camera that it was

due to the significant interest of the data controllers in the area monitored by the given camera

camera, which takes precedence over the interests of those concerned. E

regulations and documents were amended on 15 June 2020 and also on 1 October 2020,

of which the Authority has substantially reviewed the documents of 15 June 2020,

subject to the period considered.

As in the data protection authority proceedings, the Authority found an infringement

may impose a data protection fine ex officio, called on the Customer to present everything

an essential fact and circumstance which is relevant to the imposition of a fine

may. In this regard, the Customer has stated that he does not know in this form

interpret the Authority's question and asked him to indicate exactly what the facts were

you have yet to make a statement. The Client further stated that its primary interest is a

operation in accordance with the law and the avoidance of fines, so that the

complete review of the camera system and contact the Authority. The client

In its view, however, there are no significant facts and circumstances which constitute a fine

as the head of the institution during the investigation procedure

page described the cases that are raised and justified by the camera system

the need for its operation (such as fights, the careful work of carers)

proof of placement with their relatives in connection with reports of relatives, protection of property of all residents

both the preservation of the property of the Home). In addition, the Customer

it cannot list new facts and circumstances.

9

II. Applicable legal provisions

Pursuant to Article 2 (1) of the General Data Protection Regulation, the general data protection

Regulation should apply to personal data in a partially or fully automated manner

non-automated processing of personal data

which are part of a registration system or which

they want to be part of a registration system.

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

shall apply with the additions set out in

Infotv. According to Section 38 (2), the task of the Authority is to protect personal data,

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

monitoring and facilitating the enforcement of personal data in the European Union

facilitating the free movement of persons within

Infotv. Pursuant to Section 38 (2a) of the General Data Protection Decree on Supervision

authority under the jurisdiction of Hungary

in the General Data Protection Regulation and in this Act

exercised by the Authority.

Infotv. Pursuant to Section 38 (3) (b), pursuant to Section 38 (2) and (2a)

within the scope of his duties as defined in this Act, in particular at the request of the person concerned, and

ex officio data protection authority proceedings.

Infotv. Pursuant to Section 60 (1), the enforcement of the right to the protection of personal data

To that end, the Authority shall, at the request of the data subject, initiate a data protection authority procedure and

may initiate ex officio data protection proceedings.

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

Pursuant to Section 103 (1) of the Act, this Act was initiated upon ex officio proceedings

shall apply with the derogations provided for in this Chapter

Unless otherwise provided in the General Data Protection Regulation, the application was initiated

for data protection authority proceedings under Ákr. shall apply in the Infotv

with certain deviations.

According to Article 4 (11) of the General Data Protection Regulation, "" consent of the data subject "means:

voluntary, specific and well-informed and clear about the will of the data subject

a statement by which the statement or confirmation concerned is unambiguously expressed

by giving his or her consent to the processing of personal data concerning him or her. "

According to Article 5 (1) to (2) of the General Data Protection Regulation: '1. Personal data shall:

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

("legality, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not processed

in a way incompatible with those objectives; in accordance with Article 89 (1)

does not constitute incompatibility with the original purpose for the purpose of archiving in the public interest,

further processing for scientific and historical research or statistical purposes

(“Purpose-bound”).

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

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

(d) be accurate and, where necessary, kept up to date; take all reasonable measures

should be done in order to be inaccurate for personal purposes

data shall be deleted or rectified without delay ("accuracy");

10

(e) be stored in a form which permits identification of the persons concerned only

allows the time necessary to achieve the purposes for which the personal data are processed; the personal

data may be stored for a longer period only if:

archiving in the public interest for the processing of personal data in accordance with Article 89 (1)

scientific and historical research or statistical purposes,

appropriate to protect the rights and freedoms of data subjects

subject to the implementation of technical and organizational measures (‘limited

storability ”);

(f) be handled in such a way that appropriate technical or organizational measures are taken

ensure the adequate security of personal data

unauthorized or unlawful handling, accidental loss, destruction or

including protection against damage ("integrity and confidentiality").

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

to demonstrate this compliance ("accountability"). "

Under Article 6 (1) of the General Data Protection Regulation: “Personal data

is lawful only if and to the extent that it is at least one of the following

fulfilled:

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

purposes

treatment;

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

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

necessary to do so;

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

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

necessary for its protection;

(e) the processing is in the public interest or a public authority vested in the controller

necessary for the performance of the task

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

necessary, unless those interests take precedence over such interests

interests or fundamental rights and freedoms that protect personal data

necessary, in particular if the child concerned. "

Under Article 7 of the General Data Protection Regulation: '(1) Where the processing is subject to consent

the controller must be able to prove that the data subject is personal

contributed to the processing of his data.

2. If the data subject gives his consent in the form of a written declaration which is different

the request for consent is clearly excluded from these other cases

be presented in a distinguishable manner, in a comprehensible and easily accessible form, in a clear manner

and simple language. Such a statement containing the consent of the data subject shall be any such

which infringes this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The consent

withdrawal shall not affect consent-based data processing prior to withdrawal

legality. The data subject shall be informed before consent is given. THE

withdrawal of consent should be made as simple as that

entering.

(4) In determining whether the contribution is voluntary, it shall be as high as possible

the fact that, inter alia, the performance of the contract must be taken into account

- including the provision of services - is subject to such personal data

necessary for the performance of the contract. "

According to Article 13 (1) to (2) of the General Data Protection Regulation: '(1) If the data subject

personal data are collected from the data subject, the controller shall process the personal data

provide the following information to the data subject at the time of acquisition

each of them:

11

(a) the identity and contact details of the controller and, if any, of the controller 's representative;

(b) the contact details of the Data Protection Officer, if any;

(c) the purpose of the intended processing of the personal data and the legal basis for the processing;

(d) in the case of processing based on Article 6 (1) (f), the controller or

legitimate interests of third parties;

(e) where applicable, the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller is in a third country or internationally

personal data to the organization and the Commission

the existence or non-existence of a decision on compliance, or in Article 46, Article 47 or

in the case of the transmission referred to in the second subparagraph of Article 49 (1), a

to indicate appropriate and suitable guarantees and to obtain a copy thereof

reference to the methods used or their availability.

2. In addition to the information referred to in paragraph 1, the controller shall process personal data

at the time of acquisition, in order to ensure fair and transparent

provide the data subject with the following additional information:

(a) the period for which the personal data will be stored or, if that is not possible, that period

aspects of its definition;

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

access to, rectification, erasure or restriction of the processing of data, and

may object to the processing of such personal data as well as to the data subject

the right to data portability;

(c) information based on Article 6 (1) (a) or Article 9 (2) (a);

the right to withdraw consent at any time in the event of data processing,

which is without prejudice to the processing carried out on the basis of the consent prior to the withdrawal

legitimacy;

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

(e) that the provision of personal data is required by law or by a contractual obligation

is a basis or a precondition for concluding a contract and whether the person concerned is obliged to a

personal data and the possible consequences for them

failure to provide data;

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

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

understandable information on the significance of such data processing and the

the expected consequences for the data subject. "

Under Article 58 (2) of the General Data Protection Regulation: “The supervisory authority

acting in its corrective capacity:

(a) warn the controller or processor that certain data processing operations are planned

its activities are likely to infringe the provisions of this Regulation;

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

has infringed the provisions of this Regulation;

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

the exercise of his rights under this Regulation;

(d) instruct the controller or processor to carry out its data processing operations

bring this Regulation into line with the provisions of this Regulation

with its provisions;

(e) instruct the controller to inform the data subject of the data protection incident;

(f) temporarily or permanently restrict data processing, including data processing

prohibition as well;

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

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

order notification to the addressees in accordance with

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

(h) withdraw the certificate or instruct the certification body in accordance with Articles 42 and 43

revoke a duly issued certificate or instruct the certification body not to

issue the certificate if the conditions for certification are not or are no longer met;

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

in addition to or instead of the measures referred to in this paragraph; and

(j) order the flow of data to a recipient in a third country or to an international organization

suspension. "

Pursuant to Article 77 (1) of the General Data Protection Regulation, other administrative

or without prejudice to judicial remedies, any person concerned shall have the right to lodge a complaint

at a supervisory authority, in particular where he has his habitual residence, place of employment or

in the Member State of the alleged infringement, if it considers that the

processing of personal data in breach of this Regulation.

According to Article 83 (2) and (5) of the General Data Protection Regulation:

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

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

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

the amount of the administrative fine in each case

the following must be taken into account:

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

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

the extent of the damage they have suffered;

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

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

any measures taken to

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

Technical and organizational measures taken pursuant to Articles 25 and 32;

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

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

the degree of cooperation to alleviate

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

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

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

in detail;

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

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

compliance with the measures in question;

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

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

mechanisms; and

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

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

or avoided loss.

[…]

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

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

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

with the higher of the two:

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

appropriately;

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

(c) personal data to a recipient in a third country or to an international organization

Articles 44 to 49. in accordance with Article

d) the IX. obligations under the law of the Member States adopted pursuant to this Chapter;

13

(e) the instructions of the supervisory authority pursuant to Article 58 (2) and the processing of data

temporary or permanent restriction of the flow of data

non-compliance with the request or access in breach of Article 58 (1)

failure to provide.

[…] ”

Under Article 88 (1) and (2) of the General Data Protection Regulation:

1. Member States shall specify this in legislation or in collective agreements

rules may be laid down to ensure rights and freedoms

protection of employees' personal data in connection with employment

in particular recruitment for the purpose of performing an employment contract, including

fulfillment of obligations under the law or a collective agreement,

management, planning and organization of work, equality and diversity in the workplace,

health and safety at work, the property of the employer or the consumer

protection of employment-related rights and benefits, whether individual or collective

for the purpose of exercising and enjoying employment and for the purpose of terminating employment.

These rules shall include appropriate and specific measures which:

are suitable for the dignity, legitimate interests and fundamental rights of the data subject

in particular the transparency of data management, within a group or joint venture

the transfer of data within the same group of economic operators,

and workplace control systems.

[…] ”

Infotv. Pursuant to Section 71 (2): “The Authority shall, in the course of its proceedings, lawfully

may use the document, data or other means of proof obtained in another procedure. "

Infotv. 75 / A. "The Authority shall, in accordance with Article 83 (2) to (6) of the General Data Protection Regulation,

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

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

Requirements laid down in a binding act of the European Union

Article 58 of the General Data Protection Regulation

in particular by alerting the controller or processor. "

Section 9 (2) of Act I of 2012 on the Labor Code (hereinafter: Mt.)

“An employee’s right to privacy may be restricted if the restriction is a

absolutely necessary for a reason directly related to the purpose of the employment relationship and the purpose

proportionate to achieving. About the manner, conditions and expected restriction of the right to privacy

the circumstances justifying its necessity and proportionality

the worker must be informed in advance in writing. "

Mt. 11 / A. § (1): “The employee is related to the employment relationship

can be controlled over its behavior. In this context, the employer also has a technical tool

shall inform the worker in writing in advance. "

According to Section 42 (2) (a) of the Labor Code: “Pursuant to the employment contract, the employee is obliged to

to work under the direction of the employer '

Pursuant to Section 52 (1) (b) and (c) of the Labor Code: “The employee is obliged

[…]

(b) during his working hours, by the employer in order to work

be available

(c) to perform his duties in person, with the skill and care normally required,

in accordance with the rules, regulations, instructions and customs applicable to his work

[…]. ”

14

III. Decision

III. 1. General remarks

A natural person according to the definitions in the General Data Protection Regulation

face, image of personal data, viewing live image through the camera, a

taking pictures and any operations performed on personal data, such as

viewing images is considered data management.

It is related to the electronic monitoring system operated by the Client to the Authority

had to examine its data management from two perspectives. On the one hand, the residents of the Home, on the other hand

with respect to the employees of the Home.

In the present data protection authority proceedings, the Authority shall provide the Customer with a notice from 25 May 2018

until the date of initiation of the procedure, 16 July 2020

examined its data management activities related to monitoring.

III. 2. Purpose and suitability of the data processing

III. 2. 1. Purpose of data management

a) The Client has several data processing purposes in both the investigation and the data protection authority proceedings

marked for cameras.

According to the Client's statement, the purpose of data management related to camera surveillance is

Protecting the property of the home and its occupants and maintaining the rules of procedure and policy,

and the protection of human life, physical integrity, personal liberty and trade secrets.

According to the camera regulations dated June 15, 2020, the purpose of data processing by Home

the safety and security of the building, parts of buildings, premises used and monitored

protection of property, plant and equipment, valuables, valuables,

the preservation of their condition and the presence of persons, including workers, in the monitored area;

even the protection of the life, physical integrity and property of residents, business and

protection of privacy, protection of the processing of personal data, and

providing personal protection, damaging offending and abusive, aggressive

prevention of acts, detection of detected infringements, official or judicial proceedings

and the legitimate interest of the maintainer of the home to do so

complaints are investigated effectively and fully and the outcome

used for proof.

b) Due to the principle of purposeful data processing and the principle of necessity

use an electronic monitoring system or recorded by the monitoring system

recordings may be used for the following purposes in principle:

-

protection of human life, physical integrity, personal liberty,

-

protection of hazardous substances,

-

protection of business, payment, banking and securities secrecy,

-

property protection.

Property protection, business, payment, banking and securities secrecy protection, and dangerous

In the case of surveillance of substances, the controller shall certify that:

in fact, there are circumstances that justify each camera

15

and otherwise the goal to be achieved cannot be achieved. For each camera

it is also necessary for each purpose of this consideration to be performed by the data controller to ensure that the cameras

do not become a secret means of monitoring those involved, but actually the one

serve a legitimate purpose and that the purpose-based data processing is properly enforced

principle for all cameras. In the case of observations for the above purpose, it is further important

requirement that the controller pay particular attention to the

the angle of view of the camera is basically documents containing secrets on the object to be protected

to an object containing a dangerous substance and does not become

as a tool for continuous monitoring of data subjects.

c). The Authority has taken the European Data Protection Supervisor into account in its assessment of this case

Board1/2019 on the processing of personal data by video means. number

guidelines2.

According to the guidelines, in the absence of specific legislation, electronic surveillance

should be based on the rules of the General Data Protection Regulation. For personal information

they must be appropriate and relevant to the purposes of the processing, and

should be limited to what is necessary. Before installing a camera surveillance system, the

the controller must always carefully examine whether this measure is appropriate a

whether it is appropriate and necessary to achieve its objectives. That's all

In this case, camera surveillance measures may be decided if the purpose of the data processing is

by other means which are less prejudicial to the fundamental rights and freedoms of the data subject

way is not possible to achieve. In a situation such as that in the present case, if it is

the controller intends to prevent crimes against property for the purpose of protecting property

operates cameras, other types of security instead of installing a camera surveillance system

it may also take measures, such as employing security staff, porters or

you can install security locks. These measures provide equally effective protection

may provide against possible punishable acts such as camera

monitoring systems. The controller must assess this on a case-by-case basis

whether the measures could be a reasonable solution.3

Before commissioning the camera system, the data controller must assess where and when

it is absolutely necessary to use cameras.

Respect for human dignity is an absolute limit to camera surveillance.

Respect for human dignity is a requirement for fair data management

in a close context, unfair data processing practices affect not only a

protection of personal data, but also in its right to human dignity

may offend. The Constitutional Court ruled in 36/2005. stated in its decision no

electronic surveillance is therefore suitable for intrusion into the private sector,

record intimate (sensitive) life situations even in such a way that the person does not even know the

or is not in a position to consider such recordings

admissibility and their consequences. The observation made in this way is for privacy

the right to human dignity in a broader and deeper sense

it can usually affect you. The essential conceptual element of the private sphere is precisely that of the data subject

however, others should not be able to enter or view it. If you don't want to

insight is done, then not only the right to privacy in itself, but

The European Data Protection Board deals with data protection and privacy issues,

an independent European advisory body.

1

A 3/2019. Guideline number can be found at the following link:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf

2

3

3/2019. Guideline 24-25. paragraph

16

other elements of entitlement within the scope of human dignity, such as self-determination

freedom or the right to the integrity of the person may be infringed. "

Another principle for the applicability of electronic monitoring systems is also the

in the context of the right to human dignity and the principle of fair data management,

that there is no way to place a camera, especially in changing rooms, showers,

toilets, given that surveillance in these rooms is particularly violating

the right to human dignity.

III. 2. 2. Observing the inhabitants of the Home

In connection with the above data management purposes, the individual premises of the Home and in them

With regard to cameras operating mainly in the home, monitoring the Authority 's position, the

following:

(a) As explained by the Authority in its notices of inquiry, this Privacy Policy

does not consider it acceptable to use official procedures for kitchen appliances 5, 15, 18 and 21.

as they consider that they are not fit for purpose. THE

camera recording alone can only prove that someone is in some way

has taken food, but it is not possible to prove that the person is a

took food from someone else. It is dated June 12, 2020

in addition, according to the balancing test, in the kitchenettes “it is the property of the residents inside

items are in separate kitchen cabinets ’, so in the Authority’s view

without the use of cameras, the fitting of these kitchen cabinets with locks and the distribution of separate keys can ensure that

all residents have access to the Home.

protection of their property.

Regarding the fact that the cameras in the kitchenettes in the event of an emergency accident increase the

targeted intervention and the survival of carers, the Authority is of the opinion that

in the case of an emergency intervention, it is unrealistic and precisely the effectiveness of the intervention
would be reduced if you tried to view camera footage before the operation
reconstruct the circumstances of the accident. The right and fast supply of the right workforce
and an appropriate system of supervision of carers should be provided.
Data retention under Article 5 (1) (c) of the General Data Protection Regulation
appropriate for the purpose of the processing and
they must be relevant and limited to what is necessary. Given that
In the opinion of the Authority, cameras 5, 15, 18 and 21 operating in kitchenettes a
based on the above are not suitable or not suitable as defined by the Customer
data management purposes, the Authority finds that the Customer has breached the general
the principle of data protection under Article 5 (1) (c) of the Data Protection Regulation.
In relation to the issue of urgency, the Authority summarizes in point (d) of this section:
position.
(b) The Authority shall monitor the premises of the Community, including lounges
is of the opinion that cameras are not needed in these rooms either. On the one hand, because it is
According to the professional program available on the website of the home, the residents are under constant supervision.
On the other hand, in relation to the disputed events, he made a statement in relation to the purpose of:
where applicable, the Authority's position is that
that it is essential to resolve the dispute and similar situations in the future
prevention, not clarification of who applied first
to do. In addition, the Authority considers that camera surveillance is not available
in proportion to the surveillance with the aim and interest to be achieved, ie to

they observe the daily lives of residents in a suspected, rare, light-weighted case
because they can deliver justice.
Where the purpose of operating the camera system in public areas is to:

would be the protection of property, as stated by the Client in the investigation

in a letter dated 8 October 2019 stating that the cameras in the communal areas were

Focus on the assets of the home, the Authority would consider it acceptable if the

camera angle - due to the principle of purposeful data management and data saving

- to the property to be protected. For this type of relocation of the cameras, respectively

however, no changes in their viewing angles were made during the study period, and the cameras were complete

the residents of the Home are monitored in these rooms.

On this basis, the Authority concludes that the Client

in connection with cameras 3, 13, 14, 16, 17, 19 and 20 operating in lounges

breached Article 5 (1) (c) of the General Data Protection Regulation

the principle of data protection, as they are not suitable for resolving a possible dispute,

or they fix areas that are not necessary for the purpose of property protection, and they do not respond

nor the requirement of proportionality.

(c) In addition, the Authority shall review the balancing test carried out on 12 June 2020

- with regard to cameras 9, 10 and 11 in the dining room, cannot interpret that a

how cameras can help residents maintain a special diet. Position of the Authority

that cameras are specifically unsuitable for this purpose in the absence of approach to food,

there are other ways to do this that are less restrictive of the privacy of those concerned, such as

that caregivers check that the right food is given to the resident. In the kitchenettes

cameras are also unsuitable for inspecting workers due to the above.

However, as the Authority considers that the purpose of the processing itself is incomprehensible,

the processing infringes Article 5 (1) (b) of the General Data Protection Regulation

the principle of purposeful data management. In addition, Annex III to this Decision 2. As described in point 2

seriously violates the privacy rights of employees.

d) In general and in public areas in particular, such as lounges and dining rooms

protection of residents and emergency management in the context of operational cameras

the use of a camera surveillance system for the purpose of data processing

prior to this, consideration should be given to whether the purpose of the observation can be achieved by recording the recordings

without. If the resident is in danger due to his condition, then -

as explained above - there will be no retrospective review of the recorded recording

to contribute to the achievement of the purpose of data processing, as it is immediate in case of urgent care

action is required. However, in the Authority 's view, if

there is not a sufficient number of caregivers in the Home - in the community rooms

operating cameras may, where appropriate, protect the occupants if they are merely

a live image is transmitted to the monitor to which only the caregiver (s) designated for this task

so that the recordings are not recorded by any IT device. In this

in this case, the caregiver can obtain information about events in several areas - e.g.

one of the residents is in danger - where he cannot be present in person. In the absence of recording

this observation fulfills the purpose of data management on the one hand and significantly less on the other

restricts the privacy rights of data subjects. It should be emphasized, however, that this is the kind

“Viable surveillance” can only be proportionate to protect the health and lives of residents

method, the inhabitants cannot be observed for other purposes or the “viable

monitoring ”to control employees.

However, the Authority also notes in general that by the fact that the Client is individual

it intends to operate cameras again and again for several different purposes, nor does it make it legal

the purpose of the data processing or the data processing itself and does not make the specified fit

to achieve this goal.

18

III. 2. 3. Observation of Home Employees

a) During the period under review, the employees of the Home were mainly employed in the office premises

22 and 23, and - reviewing the viewing angle of the cameras sent to the Authority

9, 10 and 11 in the dining room and kitchen.

The Authority's position is as follows:

b) Pursuant to Section 42 (2) (a) of the Labor Code, the employee is an employee under an employment contract is obliged to perform work under the direction of the employer. Accordingly, the legislature adopted Mt. Section 52 (1) (b) and (c) defined as a basic obligation that a

an employee is required to be at the disposal of his employer during his working hours and to carry out his work with the expertise and diligence normally required, the rules governing his work,

carried out in accordance with regulations, instructions and customs. Retention of these legal obligations for the purpose of the legislature, Mt. 11 / A. § (1) provides an opportunity to a

employer to check the employee for his employment-related conduct.

This right necessarily goes hand in hand with the processing of personal data.

Respect for human dignity is an absolute limit to camera surveillance,

therefore, as a general rule, cameras for employees and the activities they perform are constant

cannot be operated for the purpose of monitoring without a specific purpose. It is considered illegal also the use of an electronic monitoring system aimed at employees

influencing the behavior of employees at work with the use of cameras

observation, control. The reason for this is that monitoring for control purposes may violate the principle of necessity, as the employer has a number of other ways to do so

long live Mt. 11 / A. § (1). Therefore, it cannot be

operate cameras exclusively for the benefit of workers and their

activity is observed. Exceptions are workplaces where a

the life and physical integrity of workers may be in imminent danger and may therefore be operated exceptionally camera, for example, in an assembly hall, smelter, industrial plant, or other source of danger

facilities containing It should be emphasized, however, that - the Constitutional Court

as a result of its practice - only then can a camera be operated by workers

in order to protect his life and physical integrity, if the danger actually exists and is imminent,

that is, the potential threat cannot be a constitutionally acceptable purpose for data processing.

However, all this must be proven by the employer.

It is also illegal and, where appropriate, unfair to do so

the use of an electronic monitoring system that does not have an explicit

specific purpose, but merely observes the work in general, or some

he actually uses a camera operated for other purposes to monitor workers

the employer.

In addition, the Authority considers that there is also no electronic monitoring system

nor shall it be applied in a room in which workers take a break from work

has been designated for this purpose. An exception to this may be the case if there is something in this room

there is an asset to be protected (such as a food and beverage vending machine) in connection with which

there is a demonstrable employer interest (for example, employees have repeatedly damaged the

equipment and damage had to be borne by the employer). In this case, this is the specific goal

order camera can be placed in the room, however, then the employer also

you must pay special attention to the fact that the angle of view of the camera is to be protected only

may be directed to property.

c) By contrast, in the offices of the Home according to the period under review

The angles of view of cameras 22 and 23 in operation, based on camera images sent to the Authority, are a

workers, monitoring their day-to-day activities. Position of the Authority

according to the Home and the most suitable for the protection of residents' documents, as well as money

device would be a locker or safe. If these measures do not

lead to results or are not enough, cameras can be operated as if they were

its angle of view is on the object to be protected, such as a cupboard or safe.

In the context of the problem of the payment of money, which has occurred on several occasions,

that the resident or his / her relative did not recognize him / her after signing the receipt

nor did he raise money and suspect a Home staff member or the Home that

document was forged, the Authority is also not the camera's privacy

the least restrictive solution, as it is the fact of the signature that must be proved

receipt. For example, using witnesses instead of a camera can solve the problem.

According to the statement made by the Customer in the investigation procedure, the cameras are located in the offices

and a lockable cabinet for the safekeeping of residents' money and

they focus on the safe environment. In the case of cash withdrawals, the presence of an additional person

ensure.

However, this was not substantiated by the Client in the investigation procedure

However, in contrast to the above,

In a letter received on October 10, he attached a snapshot showing Home

the faces of his co-workers were masked, not the viewing angles were changed. Above

Contrary to the statement, point 3 of the balancing test sent to the Authority, which

according to the area monitored by the cameras operating in the offices is the office itself.

In addition, the Client received the same letter to the Authority on 10 October 2020

He also stated that the head of the institution had given his written consent to the

in a courtroom, which is also his office, the camera should not be removed, or

do not change your perspective because it is in your best interest to have any

in case of suspicion of bribery or extraordinary rendition

the head of the institution himself or the Home that no such cases have occurred.

In this regard, the Authority's position is that during the period under review the Customer

he should have documented that he had indeed modified the office in this way

in the field of view of cameras operating indoors that they are specifically to be protected

which, however, has not been substantiated. Given that

following the principle of accountability, proof that the data processing

the conditions of lawfulness are in place at all times, the responsibility of the controller, which

the Customer has not complied with the certificate in respect of the present cameras 22 and 23, the Authority finds that the Customer has breached Article 5 (2) of the General Data Protection Regulation the principle of accountability under paragraph 1.

Furthermore, given that the angle of view of the cameras in the offices is not to be protected assets, the Authority finds that the Customer is unnecessary Article 5 (1) (c) of the General Data Protection Regulation. principle of data protection in accordance with

The position of the Authority is specifically set out in Article 23 of the Office of the Head of the Institution in connection with a camera is whether it is a bribe or an extraordinary placement to record, or to investigate a complaint against the head of the institution, a - the Client and the Camera Regulations, which entered into force on 15 June 2020 not suitable for audio recording - camera unsuitable. In the Authority's view, it is so abstract Without any substantiation - the purpose of the processing is not lawful because, in addition to: unsuitable for the intended purpose, raises the possibility of secret image and sound recording. The Authority notes that operating the camera for this purpose violates the general data protection regulation

20

The principle of lawful and fair processing in accordance with Article 5 (1) (a), and purposeful data processing pursuant to Article 5 (1) (b) of the General Data Protection Regulation principle.

(d) Also reviewing the balancing test conducted on 12 June 2020, and a snapshots showing the angle of view of the cameras, the position of the Authority is operating in the kitchen With regard to camera 11, its angle of view is towards workers, observing their all-day activities, which is not legal as explained above. THE In addition, the Authority considers that the balancing test is necessary on the grounds that “in the absence of a reception service, a complaint during the receipt of the goods camera is required, the camera is not suitable for this. The angle of view of the camera is all over

on the other hand, it is not suitable for checking the receipt of certain goods, on the other hand

According to the authority, it is not usually in the kitchens that the goods are received. THE

In the opinion of the Authority, an acknowledgment of receipt or the use of witnesses

desired goal.

Consequently, the Authority finds that in relation to this camera 11

data processing does not comply with Article 5 (1) (b) of the General Data Protection Regulation

the principle of purposeful data processing in accordance with

(e) The Authority shall also refer back to Annex III to this Decision. 2. In point 1 (c), the

for cameras 9 and 10 in the dining room, also states in this section that

that it is incomprehensible how cameras can help residents with a special diet

retention. The Authority considers that cameras for this purpose are specifically designed for food

in the absence of approximation, employees are unfit or also unfit for this reason

to control. However, as the Authority considers that the purpose of data processing is itself

incomprehensible, the processing infringes Article 5 (1) of the General Data Protection Regulation

(b) and infringes the principle of purposeful data management as a result of constant monitoring

personal rights of employees.

III. 3. Legal basis for data processing

1. The legal basis for the processing of data related to camera surveillance shall, in principle, be

the legal basis for a legitimate interest under Article 6 (1) (f) of the General Data Protection Regulation

may. Consent does not constitute an appropriate legal basis because its conditions are a

they are basically not valid for camera surveillance. The data controller is not

able to prove that he or she has consented to the processing of his or her personal data,

furthermore, the data subject may not withdraw his or her consent at any time.

According to the legal basis of the legitimate interest, camera surveillance is lawful if it

necessary to safeguard the legitimate interests of the controller or of a third party, unless

the interests or fundamental rights of the data subject take precedence over such interests; and

freedoms.

In a real and dangerous situation, the protection of life, physical integrity and burglary of property,

the purpose of its protection against theft or damage is legitimate for camera surveillance

may be of interest.

A 3/2019. According to Guideline No 1, a legitimate interest must actually exist and be effective

it must exist (i.e., it cannot be fictional or hypothetical). Before starting the observation

there must be an actual emergency, such as a previous incident or

serious incident. Pursuant to Article 5 (2) of the General Data Protection Regulation

In view of the principle of accountability, it is proposed that the controller record this in writing

incidents (date, method, financial loss). Incidents recorded in writing

they can serve as convincing evidence of the existence of a legitimate interest. That's right

the existence of an interest and the need for monitoring at regular intervals (a

depending on the circumstances, for example once a year)

It is important that the controller has a balance of interests to invoke the legal basis of the legitimate interest

must perform. Carrying out a balance of interests is a multi-step process that

the legitimate interest of the controller and the counterweight to the weighting must be identified

the interest of the data subject, the fundamental right concerned, must ultimately be determined on the basis of the weighting,

whether personal data can be handled. If as a result of a balance of interests

it can be established that the legitimate interest of the controller precedes the personal data of the data subjects

camera system that can be operated.

Due to the legal provisions in force and the principle of accountability, the

the controller must certify that the electronic monitoring system he uses

is compatible with the principle of purposeful data management and the outcome of the balance of interests is

resulted in the primacy of the legitimate interest of the controller.

2. In the case of employees, the legal basis of the legitimate interest is also applicable because it is the employer

(control-related) data management - in addition to camera surveillance

in general, the conditions of the legal basis for the consent cannot be met - Mt.

the nature of the employment relationship, the employee contribution

independent data management. In the context of consent, it should be noted that:

it must be voluntary as defined in the General Data Protection Regulation

be. In connection with the voluntary contribution, however, has already been repealed

the Working Party on Data Protection set up under Article 29 of the Data Protection Directive5 (a

hereinafter "the Working Party on Data Protection") has stated in several resolutions that

the voluntary contribution in an employee-employer relationship is questionable

opportunity. In the world of work, therefore, there is a different legal basis than the data subject 's consent,

the use of data processing based on the legitimate interests of the employer may be considered. The employment relationship

the proper functioning of the employer's economic activity during that period

in order to protect the privacy of workers without their consent

in limited cases, subject to warranty requirements.

This processing of data on the basis of a legitimate interest is inseparable from it

from the limits of:

-

Employer control is considered lawful if it a

absolutely necessary for a reason directly related to the purpose of the employment relationship, and

proportional to the achievement of the goal [Mt. Section 9 (2)].

-

Employer control and the tools and methods used in it are not

may violate human dignity; or the employee a

can be controlled in the context of his employment-related behavior [Mt. 11 / A. § (1)

paragraph].

-

The employee must be informed in advance of the essential requirements for data management

[Mt. Section 9 (2) and Mt. 11 / A. § (1), general data protection decree 13.

article].

3/2019. Paragraph 20 of Guideline

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

Directive 95/46 / EC of the European Parliament and of the Council

5

The Data Protection Working Party shall, prior to the date of application of the General Data Protection Regulation,

and an independent European advisory body on privacy issues, replaced by the European Data Protection Supervisor

Privacy Board has stepped in.

6

22

-

Data processing is lawful if the employer is in connection with the data processing

complies with the basic provisions of the General Data Protection Regulation: inter alia

the principle of purposeful and fair data management [Article 5 of the General Data Protection Regulation.

Article 1 (1) (a) and (b)].

The provisions of the Mt. thus provide a general authorization for the management of employer data,

however, filling these frameworks with content - the principle of accountability

is the responsibility of the employer. To the employer with the means used

detailed rules shall be laid down in the internal rules in a clear, comprehensible and precise manner,

to be defined in detail. In developing this, the employer must pay special attention

be proportionate to all data processing purposes.

3. In addition to the legal basis of the legitimate interest, the Client also based the consent of the data subject on the camera

monitoring-related data management. Effective June 15, 2020

According to the Camera Policy, this is the legal basis for the Customer’s non-home employees

applied. In view of the fact that, as mentioned above, the Authority concluded - and

NAIH / 2019/5088/4. also drew the Client 's attention in its request for a case number - that the

consent is not applicable in the case of data processing in the present case, so the Customer

in the absence of a proper legal basis, handles the personalities of those outside the Home Workers

data in the context of camera surveillance, in breach of general data protection

Article 6 of this Regulation.

The application of a legal basis for a legitimate interest requires a balancing of interests,

the first step is to map out whether the data processing is really necessary to achieve the purpose of the data controller or

whether there are alternative

solutions that can be implemented without the processing of personal data a

intended purpose.

The Authority shall amend Annex III to this Decision. Stated in point 2 that in the dining room, in the kitchen,

or in the case of cameras operating in the office of the head of the institution, the data management is not responsible

the principle of purposeful data management in kitchenettes, communal areas,

and in the case of cameras in lounges and offices, that

data management does not comply with the principle of data saving, data management is the goal

unsuitable for implementation. The suitability and necessity of the data management for the purpose a

Nor was it substantiated by a balancing test dated June 12, 2020. From the procedure

during which the Client has named several interests and several data management purposes, but it does not really turn out

what are the objective circumstances justifying the use of these cameras,

it does not follow that there is a need for camera surveillance, and

there would be no other way to achieve the goals. It also does not require data management,

if the Customer merely declares the need and that he has no other

way to achieve your goals.

Customer is subject to data management in the interest balance test dated June 12, 2020

among its necessity, defined “the image recorder is electronic

recording by the surveillance system, protection of the facility, premises, equipment,

prevention of extraordinary events, elimination of their consequences, investigation

assistance in the detection of infringements, the detection of offenders and the

protection of human life, physical integrity and personal liberty,

protection of business and payment secrets, protection of property and lawful handling of complaints

for the purpose of The operation of the camera system plays a crucial role in achieving these goals

as a significant proportion of incidents can be prevented if potential perpetrators know

that their act will be recorded by a camera, the events that have taken place, the violations,

and a significant proportion of complaints can be investigated by viewing the images. "

23

Furthermore, according to the test, “to the best of our knowledge, no such technique is available either

a solution that could be used to reconstruct what happened without taking pictures

in connection with a complaint, an accident or a possible criminal offense, so that the attainment of these

less restrictive of the right to information self-determination of data subjects

cannot be provided. Possible anonymization of the recordings, the cameras are not suitable

adjustment of the angle of view of the persons concerned would make it impossible to

the basic protection objective would not be achieved, a

without storing the recordings for a certain period of time, the data would not be available

to prove and control acts. "

In these two paragraphs of the test, the Customer lists the data management purposes, but does not

substantiates why these data processing is actually necessary and why it is not available

other solution that allows the targets without operating cameras

would be available.

Based on all this, it is not proved that the Client's interest as a data controller precedes that

the right of data subjects to the protection of personal data. Consequently, the Authority

finds that the Client has also violated the

Article 6 of the General Data Protection Regulation.

The Authority notes that the use of cameras may indeed be necessary and

can also be considered a proportionate restriction on privacy in many cases, but it is not acceptable

the approach where all processes, situations to control, control, workspace,

for surveillance of a community or residential area, camera surveillance is the response of the data controller,

for this results in the continuous observation of everyday life situations.

The need for a different method, the interest of the controller and the

a realistic assessment of the balance of interests and rights intended to be restricted, carefully

to be considered, the real need needs to be duly substantiated. In the present case,

Customer-defined interests and goals are available from cameras instead of other, private ones

no or less restrictive methods such as caring for carers

more efficient organization, increase the number of employees.

III. 4. The requirement for adequate information and transparency

As with all data management, it also applies to data management related to camera surveillance

an essential requirement is that stakeholders are appropriate, transparent and easy to understand

receive information on data processing. In this regard, the following should be considered

buy:

Both the General Data Protection Ordinance and, in the case of employees, the Mt.

that data subjects should be informed of the circumstances surrounding the processing. The general information protection

obligation set out in the Mt.

Article 13 (1) to (2) thereof

circumstances in which the controller must inform the data subject. The information

form is not specified by law, but the Authority recommends a written form

for the reason that, also following the principle of accountability, the controller must

prove that the prior information was provided.

Data management related to camera surveillance as a special data management is

employees in accordance with the system of requirements laid down in the General Data Protection Regulation

in particular, the following relevant circumstances shall be disclosed:

-

the person (legal or natural) operating the electronic monitoring system

determining

24

-

the contact details of the Data Protection Officer, if any

person

-

the location of each camera and the purpose for which it is intended

the area or subject being observed, or whether you are direct or obstructed by the camera

whether the employer carries out a fixed observation,

-

the legal basis for data processing,

-

determining the legitimate interest of the controller,

-

the storage period of the recording,

-

the range of persons entitled to access the data and whether a

to which persons and bodies the recordings may be forwarded to the

employer,

-

on the rules for reviewing recordings and whether to record recordings

what purpose the employer may use,

-

on the rights of employees in electronic communications

in the context of the monitoring system and how they can exercise their rights,

-

what their right to information self-determination will be violated

enforcement tools.

In addition, the data controller is obliged to use the camera system

place a warning sign, a so-called pictogram, in a conspicuous place.

In the Authority's view, therefore, the employer, as data controller, has electronic

surveillance system

to apply

relevant to

workers

for

provided

For each camera, you must indicate in the information sheet that it is

for what purpose you placed the camera in the given area and for what area or equipment

is the angle of view of the camera. Article 6 (1) of the General Data Protection Regulation

on the basis of the legal basis of the legitimate interest referred to in paragraph 1 (f)

why it is considered necessary to monitor the area. No

the practice whereby the employer informs the

workers to use an electronic monitoring system in the workplace.

In employment law, you know with separate information about each camera

to prove to the employer that the observation of the given area is compatible with the purpose

principle of data management and does not become a source of protection for employees,

as a means of monitoring

However, in the Authority 's view, this further information is no longer necessary a

to third parties other than employees, given that their privacy

the electronic monitoring system is less affected or affected by these persons

be aware of the area or property that the camera is monitoring,

the system would lose its security function. As a result, outside of employees

general information without detailed description of each camera

obligation on the controller.

With regard to information provided to third parties other than employees a

The Authority also draws attention to the European Data Protection Board's 3/2019. number

guidelines for both first and second line information

conditions, their recommended form, and the operation of the cameras

data security requirements.

25

The Client, though, placed warning signs about the camera surveillance and examined it

Although it amended its data management information for the period 15 June 2020, it

still does not comply with the general data protection regulation

requirements, as it does not or does not adequately include:

-

determination of the legitimate interest. The prospectus only states that

The legal basis for data processing is based, in part, on the legitimate interest of the controller

a balancing test has also been made to support this, but that is exactly what is legitimate

interest, it does not appear in the prospectus;

-

the range of persons entitled to access the data and whether the recordings

to which persons and bodies, in which case they may be transmitted;

-

the rules for reviewing the recordings and that the recordings

what purpose it can be used for;

-

the rights of employees and other stakeholders in electronic communications

in the context of a monitoring system and how they can exercise their rights.

The prospectus only lists the rights of affected persons in the Information Act. Present

However, the rules on data management are set out in Infotv. instead of the general

contained in the Data Protection Regulation, including the general rules on the rights of data subjects

the rights of data subjects under the Data Protection Regulation and the way in which they are exercised

provide information. Data subjects are entitled to in connection with data management

In the information on the rights, the Client must specify what

through contact details, the person can submit the application, how much the data controller

comply with the data subject's request within a reasonable time. In addition, it is advisable to explain the individual

the content of the rights is also affected, as individual rights are named by individuals

may not be known. In addition, the Customer must exclude the data subject

certain aspects of the exercise of the law;

-

the nature of the data subject's infringement of their right to information

enforcement tools. Customer's enforcement

Among the options, it is worth mentioning above all that the data subject

before initiating any proceedings, it is advisable to file a complaint with the Customer,

send it to the data controller to have the data controller automatically restore the lawful

condition. There are two procedures available to the Client for enforcement

should provide information on the possibility of initiating On the one hand, it must be up

draw the attention of the data subject to the fact that the Authority may initiate proceedings. The

Customer must indicate in the prospectus the Authority's official electronic collection

address, postal contact details, telephone number and the address of the website of the Authority.

On the other hand, the data subject must be informed of the possibility of going to court. In this

In this case, the Client must take into account the specificity that the data subject may decide to

to institute proceedings in the courts for the place where he is domiciled or resident.

In addition to these shortcomings, the prospectus erroneously states that the data management is

the legal basis of the data processing is set out in Annex III to this Decision. Point 2

legitimate interest of the controller.

Furthermore, the information and the balancing test are not in line with the

camera policy, as it has a retention period of 10 days, as opposed to

10 working days as specified in the prospectus - and the balancing test.

It is not included in the prospectus in addition to the employees subject to each camera

and their purpose, the area, the subject, the

or whether it is live or recorded with that camera

whether the employer is monitoring.

26

Furthermore, the fact that data management does not comply with data protection requirements does not comply with the data

protection requirements

transparent, data management information is difficult to understand because a

in addition to the prospectus, several different documents, the camera regulations and the balance of interests

they should select the relevant information from the test to map out what

they become the subjects of a data management process. They can only do this if a

in addition to information available to anyone, the regulations and the balancing test are requested

these two documents are not available on their own.

However, the information is considered adequate and transparent if it is uniform

data management information contains the general data protection guidelines for data management

information in accordance with Article 13 (1) to (2) of

the person entering the building can access and get to know him before entering.

Fairness under Article 5 (1) (a) of the General Data Protection Regulation and

principle of transparency, in accordance with the provisions of the General Data Protection Regulation (39)

requires the processing of personal data

information is easily accessible and comprehensible and that it is clear and

they are worded in simple language. This principle applies in particular to those concerned with

the identity of the controller and the purpose of the processing

for further information in order to ensure the fair and personal disclosure of the data subject 's personal data

transparent treatment and the information that data subjects have a right

receive confirmation and information about the data processed about them. Consequently, it is

under the General Data Protection Regulation, it complies with the data protection requirements if

information on data management is contained in a document covering data management

all the circumstances referred to in Article 13 (1) to (2) of the General Data Protection Regulation.

Based on all this, given that it was not included in the Customer's data management information

in a transparent and transparent manner

information, the Authority finds that the Customer has violated the general data protection

the principle of transparency under Article 5 (1) (a) of the Regulation and the general data protection

Article 13 (1) to (2) of that Regulation.

III. 5. Sanctioning

1. The Authority shall act in accordance with Article 58 (2) (b) of the General Data Protection Regulation

found that the Customer had infringed Article 5 (1) of the General Data Protection Regulation

the principle of purposeful data processing pursuant to paragraph 1 (b) on the grounds that it is for an unlawful purpose

operated cameras 9, 10, 11 and 23 during the period under review; violated the

the principle of data protection under Article 5 (1) (c) of the General Data Protection Regulation

by operating cameras 5, 15, 18, and 21, and by operating the

3, 13, 14, 16, 17, 19, 20, and 22 that they were unsuitable, respectively

unsuitable for achieving the data management purpose specified by the Customer; also violated

the principle of accountability under Article 5 (2) of the General Data Protection Regulation

by failing to justify a change in the angle of view of cameras 22 and 23; violated

lawful under Article 5 (1) (a) of the General Data Protection Regulation and

the principle of fair data management is the 23rd camera located in the office of the head of the institution

operation; infringed Article 6 of the General Data Protection Regulation by not

handles the personal data of data subjects under camera surveillance on an appropriate legal basis

context; infringed Article 5 (1) (a) of the General Data Protection Regulation

principle of transparency and Article 13 (1) to (2) of the General Data Protection Regulation,

as the camera did not provide adequate and transparent information to those concerned

monitoring-related data management;

27

2. The Authority shall act in accordance with Article 58 (2) (d) of the General Data Protection Regulation

instructed the Customer to - with the exception of Cameras 5, 15, 18 and 21

that they have already been decommissioned by the Customer - terminated without a legitimate aim

operated cameras or adjust their viewing angles to suit a

requirements for lawful data management; and to operate it on an appropriate legal basis

cameras that have been used for legitimate purposes and are not objectionable by the Authority

and provide adequate and transparent information on them.

3. The Authority has examined whether a data protection fine against the Client is justified

imposition. In this context, the Authority shall comply with Article 83 (2) and (3) of the General Data Protection Regulation

Infotv. 75 / A. § considered all the circumstances of the case and found that a

in the case of infringements detected in the present proceedings, the warning is neither proportionate nor appropriate

a dissuasive sanction, it is therefore necessary to impose a fine.

By imposing fines, the Authority's specific preventive purpose is to encourage the Client

to consciously continue its data management activities and activities, giving the

necessary for data subjects to exercise control over the processing of their personal data

information. And usually all data controllers in a similar situation are needed

make it clear to the public that the processing of personal data requires increased awareness,

it is not possible to take any proactive measures in this area on the basis of common sense

operate without carelessly trusting that there will be no inconvenience to personal information

actually out of control. Such negligent conduct protects the rights of those concerned

ignores it and, as such, cannot go unpunished [general privacy

Article 83 (2) (b) of the Regulation].

In setting the amount of the fine, the Authority took into account, in particular, that:

Infringements committed by the Customer are covered by Article 83 (5) of the General Data Protection Regulation

an infringement falling within the higher category of fines under points (a) and (b)

are considered.

The Authority took into account as an aggravating circumstance that:

-

the long time of the infringements, the start of the investigation procedure - 28 May 2018

Have existed since and in part still exist [Article 83 of the General Data Protection Regulation.

Article 2 (2) (a)];

-

the infringement concerned a large number of data subjects, dated 12 June 2020

according to the balancing test, 40 employees and 82 employees, and - smaller

to the extent that no additional turnaround at home can be quantified

concerns third parties [Article 83 (2) (a) of the General Data Protection Regulation

point];

-

data management employees who have a hierarchical relationship with the Customer, and

Affects elderly and vulnerable people living at home [general

Article 83 (2) (a) of the Data Protection Regulation];

-

Article 58 (2) of the General Data Protection Regulation

(b) and (d) of the Infotv. Section 56 (1) - three

repeatedly called on the Customer to terminate its data processing, respectively

take measures to ensure the lawful processing of data, the obligation of which is

Customer did not comply or only partially complied with [Article 83 (2) of the General Data Protection Regulation

paragraph (e), (d) and (i)].

The Authority took into account as an attenuating circumstance that

-

the Customer has taken steps after initiating the data protection authority proceedings and

also appointed a lawyer to ensure lawful data management and out of order

28

placed cameras 5, 15, 18, and 21 installed in kitchenettes [general

Article 83 (2) (c) and (f) of the Data Protection Regulation];

-

the Authority has exceeded the administrative deadline [Article 83 (2) of the General Data Protection Regulation

paragraph (k)].

The Authority did not consider the general rule to be relevant in setting the amount of the fine

circumstances under Article 83 (2) (g), (h) and (j) of the Data Protection Regulation, as

they cannot be interpreted in the context of a particular case.

In the light of the above, the Authority will set the amount of the fine at the minimum

close to.

According to the public report of 2019, the current year is available for tax purposes

The result was more than HUF 29,000 thousand, so the data protection fine imposed does not exceed

maximum fine that may be imposed.

ARC. Other issues:

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

The present decision of the Authority is based on Art. 80-81. § and Infotv. It is based on Section 61 (1). THE decision of the Ákr. Pursuant to Section 82 (1), it becomes final upon its communication. The Ákr. Section 112 and § 116 (1) and (4) (d) and § 114 (1)

there is an administrative remedy against the decision.

***

The Ákr. Pursuant to Section 135, the debtor is in arrears at a rate corresponding to the statutory interest he is obliged to pay a supplement if he fails to meet his obligation to pay money on time.

The Civil Code. 6:48. § (1), in the case of a debt owed, the debtor is in arrears valid on the first day of the calendar half-year affected by the delay shall pay default interest at the same rate as the basic interest.

The rules of administrative litigation are laid down in Act I of 2017 on the Procedure of Administrative Litigation (a hereinafter: Kp.). A Kp. Pursuant to Section 12 (1) by decision of the Authority The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (3) Pursuant to subparagraph (a) (aa), the Metropolitan Court has exclusive jurisdiction. A Kp. § 27 Paragraph 1 (b) in a dispute in which the tribunal has exclusive jurisdiction competent, legal representation is mandatory. A Kp. Pursuant to Section 39 (6), the application has no suspensory effect on the entry into force of the administrative act.

A Kp. Section 29 (1) and with regard to this, Act CXXX of 2016 on Civil Procedure. applicable in accordance with Section 604 of the Act, electronic administration and trust services CCXXII of 2015 on the general rules of According to Section 9 (1) (b) of the Act no the client's legal representative is obliged to communicate electronically.

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

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

based on.

29

On the reintroduction of certain procedural measures in the event of an emergency

112/2021. (III. 6.) of the Government of the Republic of Hungary (hereinafter: Veir.), If this decree

the tightening of the defense does not affect the running of the time limits. Section 36 (1) - (3) of the Act

During the period of enhanced defense, the court shall act out of court, including

review procedures. If a hearing were to be held or requested by either party,

or a hearing has already been scheduled, the trial court will notify the parties out of turn at the hearing

and give the parties the opportunity to make their statements in writing

put forward. Should a trial be held outside the time of the defensive defense,

the plaintiff may then request the court to hear the trial in lieu of an out-of-court settlement

postpone the date of termination of the enhanced defense if:

has not ordered, at least in part, the suspensory effect of an administrative act,

bringing an action has suspensory effect and the court has not ordered the suspension of the suspensory effect

(c) no interim measure has been ordered.

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

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

the Itv. Section 59 (1) and Section 62 (1) (h) shall exempt the person initiating the proceedings

half.

If the Applicant does not duly prove the fulfillment of the required obligation, the

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

if the Applicant has not complied with the obligation set out in the final decision of the authority,

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

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

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

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

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

implements. Infotv. Pursuant to Section 61 (7) of the Authority,

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

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

implements.

Budapest, March 25, 2021

Dr. Attila Péterfalvi

President

c. professor