Case number: NAIH-88-13/2022.

History: NAIH-8968/2021.

Subject: decision

H A T A R O Z A T

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

applicant (hereinafter: Applicant) on 10 December 2021 with […] (hereinafter:

Respondent) opposite, with the cameras installed by the Respondent in its business premises at […]

in connection with illegal data processing, to establish and terminate it, and personal data

the following decisions in the data protection authority proceedings initiated following his request for deletion

brings:

I. In its decision, the Authority grants the Applicant's request and states that a

The respondent has violated natural persons regarding the handling of personal data

on the protection and free flow of such data, as well as the 95/46/EC Directive

2016/679 (EU) regulation on externalization (hereinafter: the general data protection

Regulation) Article 6 (1)

II. The Authority obliges the Applicant to review its data management and the data management

The following brings its operations into line with the provisions of the General Data Protection Regulation

according to:

1. Eliminate illegal data processing on the one hand by stopping the cameraman

audio recording with a surveillance system, on the other hand, not at all during opening hours

operates the camera system, in addition

2. in addition to the above illegal data processing, in relation to data processing that can be made legal

bases the data management on an appropriate legal basis, the consideration of interests necessary for it

completed in compliance with Article 6 (1) point f) of the General Data Protection Regulation

according to the requirements of the legal basis, as well as provide the affected parties with the general

appropriate data management information according to Article 13 (1)–(2) of the Data Protection Regulation,

obsession

3. completely stop data processing in connection with the examined cameras!

III. The Authority rejects the request to delete the Applicant's personal data.

ARC. In its decision, the Authority ex officio states that the Respondent has violated the

Article 13 (1)-(2) of the General Data Protection Regulation.

The Authority is the I. and IV. due to legal violations established in point - with the fact that another data protection

in the event of a violation of the law, when determining the legal consequences, the present violation, as

history will be taken into account with increased weight - he gives a warning.

The II. to the Respondent from the decision becoming final

must be in writing within 30 days - together with the submission of supporting evidence

- certify to the Authority. In case of non-fulfillment of the obligation, the Authority shall issue a decision

implementation.

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

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

can be challenged in a lawsuit. The statement of claim must be submitted to the Authority electronically1, which

forwards it to the court together with the case documents. The request for the holding of the trial is submitted by the

must be indicated in the application. For those who do not receive full personal tax exemption a

the fee for the judicial review procedure is HUF 30,000, the lawsuit is subject to the right to record the fee. THE

Legal representation is mandatory in proceedings before the Metropolitan Court.

I N D O C O L A S

I. Procedure of the procedure

infringement, i.e. without permission

The Applicant submitted an application to the Authority on December 10, 2021, in which the

He objected to the camera system installed by the respondent at the business premises at […]. THE

attached the photo taken from the cameras to the application.

In his application, the Applicant submitted that the business premises operated by the Applicant are external

with cameras mounted on the wall, by moving them as the public space and the Applicant's address

marked […]. is also monitoring the movements of the residents of the apartment building at no.

The Authority NAIH-8968-2/2021. in order no. With reference to § 44, the

Applicant to make up the gaps in the application. The Applicant dated January 27, 2022, to the Authority

In his letter sent by post, received on February 1, he clarified his request and asked the

equipped

Authority to determine the

personal data obtained during surveillance with a camera system

unauthorized

management, and also instruct the Applicant about the personal data managed by the camera system

delete it, or instruct the Applicant to perform its data management operations

in accordance with the provisions of the decree. The Applicant also supplemented his application with the following

with the data required to identify the data controller, as well as clarified by the data subject

quality, in connection with which he submitted that he lives in the property at […], to whom

in this way, he obtained his personal data during surveillance with the objected camera system

managed by the Applicant. The Applicant attached photographs of the location of the cameras and the

from the area monitored by cameras.

The Applicant is NAIH-88-1/2022. No., in the form of an email dated January 1, 2022

in his submission, he supplemented the contents of his application, as well as 3 pieces, the cameras

attached a photo illustrating the position for the Authority.

At the same time, considering that the Applicant sent his submission to the Authority in the form of e-mail

submitted, the Authority called on the Applicant in order number NAIH-88-2/2022 to

declarations by post or in person or via the e-Paper service in the possession of the customer portal

submit it to the Authority via

1 The NAIH_KO1 form is used to initiate the administrative lawsuit: NAIH KO1 form (16.09.2019) The form is the general

can be filled out using a form filling program (ÁNYK program).

In view of the Petitioner's submission, the Authority invited the Petitioner to make a statement

in order to clarify the facts, to which the Respondent submitted a response in March 2022

It was received by the Authority with the date of 1

Given that the Authority had additional questions based on the Respondent's statements

up, in order to establish the facts, again in the order of NAIH-88-6/2022

invited the Applicant to make a statement.

The Respondent's response was received by the Authority via the e-Paper service.

In an order, the Authority informed the parties about the completion of the evidence procedure and called the

parties to exercise their right to make a statement within the deadline specified in the order, respectively

they can exercise their right to inspect documents.

The Applicant sent a new submission to the Authority under registration number NAIH-88-10/2022,

in which he presented that he recorded the recordings using the camera system he operated

seized by the […] department of the […] Police Headquarters, for verification of which by the Authority

sent the decision on this, as well as minutes.

The Applicant submitted a document inspection request, to which the Authority sent the documents by post

approved at the same time as sending

The Applicant did not present any new evidence other than what was revealed in the evidentiary procedure,

moreover, he did not make a motion for proof.

II. Clarification of facts

on recordings a

the entrance to the condominium is not

The Respondent submitted that it was the Respondent who decided to install the camera system

the protection of the physical integrity of the guests and staff of the business premises, as well as the one placed on the

terrace

due to the protection of assets, in order to protect a vital interest. As the Applicant

stated that the movement of the apartment building is not monitored in any way, with the camera system

recorded

it seems In his submission, he submitted that

does not keep data management records, given that they are smaller than 250 people, or

they do not manage special data. Two […] type devices were installed, which are IP

cameras, they have internet access, so they can also view the cameras from a mobile phone

his pictures. In its submission, the Applicant stated that it does not have a camera system

operating central computer, the camera records 32 GB in its internal memory,

approximately 4 daily recordings, as well as a sound track for the image recordings, in the same way

stored.

In his submission, the Applicant also informed the Authority that the recordings will not be provided

to the public, at the same time, if a crime is suspected, the recordings in question are

it will be saved until the end of the official procedure, it will be handed over in the event of an official request, to which earlier

there was already an example, thereby helping the investigation.

The Respondent submitted that since the system is not open source, directly to the streams

the Applicant cannot access it. The online or saved data of the cameras are available from the Internet.

Authentication is handled by the server of the camera manufacturer, after which a P2P connection is established with the

camera

and the mobile application used for viewing. The Respondent stated that a

recordings will not be forwarded in the absence of an official request, and everything about data management

you can request information from all the contact details of the company concerned. In addition to his application, the Applicant

attached two photographs of the images taken by the cameras, on which the catering terrace

visible from two different angles, based on footage taken on March 1, 2022. Based on the recordings a

The authority found that the entrance to the apartment building is not in the camera's field of view,

however, the public area in front of it (sidewalk section) does.

Furthermore, in his reply received on April 4, 2022, the Respondent submitted that the legitimate interest
did not prepare an interest assessment test to support it, however, if requested by the Authority, then
will be prepared immediately. The public space in front of the business premises is a
[…] It is rented from the municipality
Applicant, as proof of which he attached to the Authority the usage certificate dated […]
agreement. According to the usage agreement, the user is given the geographical number […]
public space, among other things, on the condition that the sidewalk
in the case of relocation, a pedestrian corridor of at least 1.5 m must be maintained.
The Authority found that the usage agreement and the submitted blueprints
based on - according to the calculations, the area occupied by the terrace furniture is released for use
taken area - the use does not extend to the 1.5 meter pedestrian corridor, only the shop
to the area in front of the entrance and beyond the pedestrian corridor, specifically by the tables and chairs
to an occupied area.
occupying territory,
The Applicant submitted in his submission that the agreement and the relevant municipal
However, the regulations do not specify the exact location of the terrace, so it is not known on the recording either
to check. Defined in the deed
at least one and a half meters
by leaving a pedestrian corridor free, the exact location of the terrace can be changed. The catering
due to its characteristics (e.g. guests push several tables together), the area cannot be precisely defined.
The Applicant also attached to his submission, before concluding the usage agreement, that
blueprints submitted to the municipality, as well as the opinion of [...] the chief architect. He added
also, to your letter, the photos taken from the cameras, which do not have an exact model designation
can be found, however, the Applicant stated that based on the images found on the Internet
their type can be clearly identified.
The Respondent submitted that the camera surveillance system is provided verbally and, upon request, in writing

in addition to information, with the pictogram and description on the door, as well as in their drink menus

at the same time, they inform the affected parties with the same pictogram and text also placed

so far no one has asked for detailed information. He attached it to the Respondent's submission on the door

placed informative picture, on which the following text can be read:

"We have a camera surveillance system in our bar and terrace for the safety of all of us

works which sound

delete it.

Regarding data protection a

further

information."

The Applicant also submitted the letter dated […] to the […] department of the […] Police Headquarters

decision. According to this, in front of [...] at […] - the relevant entrance of which is […]

located on the street - in progress due to the suspicion of the crime of theft committed with violence against property

recordings made by the camera system operated by the Applicant in the criminal case

it was seized by the […] Department of the […] Police Department. The Respondent attached to his letter [...]

dated, also the protocol issued by […] Police Headquarters […] Department […] Subdivision.

III. Applicable legal provisions

recordings automatically after 4 days

[…], or you can ask our staff

records. THE

too

Article 2 (1) of the General Data Protection Regulation applies to personal data

partially or fully automated processing, as well as their personal

for the non-automated processing of data that is part of a registry

are part of a system or are intended to be part of a registration system. The

information self-determination for data management under the scope of the General Data Protection Regulation

CXII of 2011 on law and freedom of information. Act (hereinafter: Infotv.) § 2

According to paragraph (2), the general data protection regulation must be amended with the additions indicated there apply.

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

in order to do so, the Authority initiates an official data protection procedure at the request of the data subject and may initiate official data protection proceedings ex officio.

In the absence of a different provision of the general data protection regulation, the data protection authority for procedure CL. 2016 on the general administrative procedure. law (hereinafter: Ákr.) shall be applied with the deviations specified in Infotv.

Pursuant to Article 2 (2) of the General Data Protection Regulation, the regulation does not applies to the processing of personal data if:

a) they are carried out during activities outside the scope of EU law;

b) the member states carry it out during activities falling within the scope of Chapter 2 of Title V of the EUSZ;

c) carried out by natural persons exclusively in the context of their personal or home activities;

d) prevention, investigation, detection and prosecution of crimes by the competent authorities conducted for the purpose of conducting or enforcing criminal sanctions, including public safety protection against threats and the prevention of these threats.

Based on recital (18) of the general data protection regulation, the regulation does not shall apply to the personal data provided by the natural person exclusively as personal data for treatment carried out in the context of home activities, which are therefore of no professional or business nature cannot be associated with the activity. It is considered a personal or home activity for example, correspondence, address storage, and personal and home activities mentioned contact and online activities on social networks. E regulation must be applied, however, to those data managers and data processors who a for the processing of personal data in the context of such personal or home activities is

tools are provided.

According to recital (46) of the General Data Protection Regulation, data management also

shall be considered lawful when it is the life of the person concerned or other mentioned above

it is done to protect the interests of a natural person. Another natural person is vital

with reference to his interests, personal data processing may in principle only take place if

revolving data processing cannot be carried out on other legal bases. Some types of personal data management

can serve important public interests and the vital interests of the data subject at the same time, for example,

in the event that the data is processed for humanitarian reasons, including when epidemics and

to monitor their spread, or in a humanitarian emergency, especially a natural one

it is necessary in case of man-made disasters.

According to Article 4, Point 1 of the General Data Protection Regulation, personal data is the identified or

any information relating to an identifiable natural person ("data subject"); it is possible to identify the a

natural person who directly or indirectly, in particular an identifier,

for example name, number, location data, online identifier or the natural person's physical,

one concerning his physiological, genetic, intellectual, economic, cultural or social identity

or can be identified based on several factors.

According to Article 4, Point 2 of the General Data Protection Regulation, data management of personal data

or any operation performed on data files in an automated or non-automated manner

or a set of operations, such as collection, recording, organization, segmentation, storage, transformation

or change, query, insight, use, communication, transmission, distribution or

in other ways

accessible

by lot, alignment or connection,

restriction, deletion or destruction.

5

Pursuant to Article 4, Point 7 of the General Data Protection Regulation, the data controller a

natural or legal person, public authority, agency or any other body that a

the purposes and means of processing personal data independently or together with others

define; if the purposes and means of data management are determined by EU or member state law

and, the data controller or the special aspects regarding the designation of the data controller in the EU

or may be determined by the law of the member state.

Based on Article 5 (2) of the General Data Protection Regulation, the data controller is responsible for (1)

for compliance with paragraph and must also be able to demonstrate this compliance

("accountability").

Management of personal data pursuant to Article 6 of the General Data Protection Regulation

it is only legal if and to the extent that at least one of the following is fulfilled:

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

for its treatment;

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

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

required;

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

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

necessary for its protection;

e) data processing is in the public interest or for the data controller

necessary for the execution of a task performed in the context of its exercise;

vested public authority

driver's license

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

necessary, unless the interests of the data subject take precedence over these interests

or fundamental rights and freedoms that require the protection of personal data,

especially if a child is involved.

Based on Article 13 (1)-(2) of the General Data Protection Regulation:

"(1) If personal data concerning the data subject are collected from the data subject, the data controller a

obtaining personal data

at the time of making it available to the person concerned

all of the following information:

a) the identity and contact details of the data controller and, if any, the representative of the data controller;

b) contact details of the data protection officer, if any;

c) the purpose of the planned processing of personal data and the legal basis of data processing;

d) in the case of data management based on point f) of paragraph (1) of Article 6, the data controller or

legitimate interests of third parties;

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

transmit personal data,

f) where appropriate, the fact that the data controller is a third country or an international organization

wishes for

and compliance of the Commission

existence or absence of its decision, or in Article 46, Article 47 or Article 49 (1)

in the case of data transfer referred to in the second subparagraph of paragraph

indication of guarantees, as well as the methods for obtaining a copy of them or that

a reference to their availability."

6

"(2) In addition to the information mentioned in paragraph (1), the data controller is the personal data

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

ensure, informs the data subject of the following additional information:

a) on the period of storage of personal data, or if this is not possible, this period

aspects of its definition;

b) the data subject's right to request from the data controller the personal data relating to him

access to data, their correction, deletion or restriction of processing, and

you can object to the processing of such personal data, as well as to the data portability concerned

about his right;

c) based on point a) of Article 6 (1) or point a) of Article 9 (2)

in the case of data management, the right to withdraw consent at any time, which

it does not affect the legality of data processing carried out on the basis of consent before the withdrawal;

d) on the right to submit a complaint to the supervisory authority;

e) that the provision of personal data is a legal or contractual obligation

is based on or a prerequisite for concluding a contract, as well as whether the person concerned is obliged to the personal

provide data,

it can work

failure to provide data;

with their possible consequences

also what it's like

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

also profiling, and at least in these cases to the applied logic and that

comprehensible information regarding the significance of such data management and the data subject

looking at the expected consequences."

Infotv. 60/A. According to § (1), in the official data protection procedure, the administrative

a deadline of one hundred and fifty days, which does not include the deadline necessary to clarify the facts

the time from the invitation to provide data to its fulfillment.

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

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

operations in connection with general data protection

defined in the decree

may apply legal consequences.

According to Article 58(2)(b) of the General Data Protection Regulation, the supervisory authority
condemns the data manager or data processor if its data management activities have violated it
the provisions of this regulation, and pursuant to point d) of the same paragraph, the supervisory authority
acting within its corrective powers, instructs the data controller that its data management operations - given
in a specified manner and within a specified period of time - harmonises this regulation
with its provisions, and also according to point g) of Articles 16, 17 and 18
properly orders the correction or deletion of personal data, as well as the data management
its limitation, and in accordance with Article 17 (2) and Article 19, orders that
the notification of the recipients to whom the personal data has been disclosed.
According to Article 83 (1) of the General Data Protection Regulation, all supervisory authorities
ensures that due to the violation mentioned in paragraphs (4), (5), (6) of this regulation, this article
administrative fines imposed on the basis of each case are effective, proportionate and
be deterrent.
According to Article 83 (2) of the General Data Protection Regulation, the administrative fines are
depending on the circumstances of a given case, referred to in points a)-h) and j) of Article 58 (2)
must be imposed in addition to or instead of measures. When deciding whether it is necessary

for the imposition of an administrative fine, and when determining the amount of the administrative fine
in each case due consideration shall be given to the following:
a) the nature, severity and duration of the infringement, taking into account the data management in question
nature, scope or purpose, as well as the number of persons affected by the infringement, as well as the
the extent of the damage they have suffered;
b) the intentional or negligent nature of the infringement;
c) mitigating the damage suffered by the data controller or the data processor
any action taken in order to;
d) the degree of responsibility of the data manager or data processor, taking into account the 25.

and technical and organizational measures taken pursuant to Article 32;

e) relevant violations previously committed by the data controller or data processor;

f) with the supervisory authority to remedy the violation and the possible negative effects of the violation

extent of cooperation to mitigate;

g) categories of personal data affected by the infringement;

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

whether the data controller or the data processor reported the violation and, if so, how

with detail;

i) if against the relevant data manager or data processor previously - in the same a

subject - one of the measures mentioned in Article 58 (2) was ordered, a

compliance with said measures;

j) whether the data controller or the data processor considered itself approved according to Article 40

to codes of conduct or approved certification mechanisms pursuant to Article 42;

as well as

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

financial benefit gained or avoided as a direct or indirect consequence of the infringement

loss.

According to Article 83 (5) a) and b) of the General Data Protection Regulation The following

violation of provisions - in accordance with paragraph (2) - a maximum of EUR 20,000,000

with an administrative fine in the amount of, or in the case of enterprises, the entire previous financial year

must be hit with an amount of no more than 4% of its annual world market turnover, with the two

the higher amount must be imposed:

a) the principles of data management - including the conditions of consent - of Articles 5, 6, 7 and 9

appropriately;

b) the rights of the data subjects in Articles 12–22. in accordance with article

Based on Article 30 (1) of the General Data Protection Regulation, all data controllers and - if any

such - the data controller's representative is responsible for data processing

keeps records of activities. This register contains the following information:

a) the name and contact information of the data controller, as well as - if there is one - of the joint data controller, i.e

the name and contact information of the representative of the data controller and the data protection officer;

b) the purposes of data management;

c) description of categories of data subjects and categories of personal data;

8

d) categories of recipients to whom the personal data is or will be communicated, including a

recipients in third countries or international organizations;

e) where applicable, personal data to a third country or international organization

information regarding the transmission, including third country or international

identification of the organization, as well as according to the second subparagraph of Article 49 (1).

in the case of transmission, a description of the appropriate guarantees;

f) if possible, the deadlines for erasing the various data categories;

g) if possible, the technical and organizational measures referred to in Article 32 (1).

general description.

Budapest Capital IX. 3/2016 of the Board of Representatives of Ferencváros District Municipality. (I.

29.), Budapest Capital IX. Owned by the Ferencváros Municipality

According to § 2 (1) of the local government decree on the use and order of public spaces, "The public space

for non-intended use (a

owner

consent, and the conclusion of the contract including the consent (hereafter together:

public space use consent) is required. Use of public space other than intended

is defined as any type of use that is common to public areas by society

use that is different from its accepted or usual everyday use function

results in It is present to make ownership decisions related to the use of public land

according to the provisions of the decree, the Mayor and

the City Management Committee is entitled."

hereinafter: use of public space) a

ARC. Decision

IV.1. The person of the data controller

Pursuant to Article 4, point 7 of the General Data Protection Regulation, a data controller is a natural or legal person

person […], which independently determines the purposes and means of personal data management

together with others it determines […].

In the statements submitted to the Authority by the Applicant - as the operator of the camera system -

clearly identified himself as the data controller and, according to the Respondent's statements, the camera

installed it yourself. As the person determining the purpose and means of data management, the Requested

on the basis of Article 4, point 7 of the GDPR, the Authority considered it a data controller.

IV.2. Legality of camera data management

Based on the General Data Protection Regulation, the image of the data subject is considered personal data.

Affected is identified or identifiable

natural person. According to all this,

if a natural person can be identified based on a recording, then the photo recording

is personal data, taking pictures is considered data management.

proof that the data management

According to Article 5 (2) of the General Data Protection Regulation, it is essentially the data controller

accountability articulating objective responsibility and enhanced care requirements

arising from its basic requirement, the obligation of the Requested as a data controller

conditions - data management

of that

from the beginning -

by

for monitoring, which for the data controller is a continuous access to the private sphere of the data subjects
provides an opportunity for intervention. The data controller can only reasonably trust that everything
complies with the legal requirements of data management, if the obligation to certify this
it can satisfy, and it is sufficient for the Authority, the trial court, and the person concerned
this is true with the camera
exist. In particular
its legality
continuously
9
can demonstrate the existence of these conditions in a way that provides certainty.
It follows that if the data controller cannot prove that the data subject has objected
its data management would have met the data protection requirements during the examined period, it does not
meets the basic requirement of accountability, thereby violating the general
Article 5 (2) of the Data Protection Regulation. For data controllers, from the planning of data management
starting from the start of data management, up to the deletion of the processed personal data
they must implement all data management operations in such a way that they can prove at any time
how they complied with data protection regulations. Based on the principle of accountability, it is
during the entire process of data management, data controllers must implement the data management
compliance with data protection rules
operations that they can
to prove it. The principle of accountability,
at the process level
can be interpreted, all specific data management activities of a specific data subject are personal
also applies to the processing of your data.
so not only in general,
On the basis of accountability based on Article 5 (2) of the General Data Protection Regulation

the data controller is obliged to document and record the data management in such a way that it

its legality can be proved afterwards

important

requirement that the documentation refers to the data controller and its data management

be prepared, because it is not clear from the mere literal adoption of the legal texts

why this data management is necessary.

be. From the principle of accountability

arising

The 3/2019. European Data Protection Board guideline 2 (hereinafter: Guidelines)

notes that video camera surveillance can serve many purposes, such as real estate and others

support for property protection, support for the protection of human life and physical integrity or

collection of evidence related to a civil claim. In principle, according to Article 6 (1).

any legal basis can serve as a basis for the processing of data through video camera surveillance

regarding.

In practice, however, the most common characteristics stem from the nature of the examined data management

due to this, the following provisions related to the camera surveillance system can be referred to

in relation to data management:

• point f) of paragraph (1) of Article 6 (legitimate interest),

• point e) of Article 6 (1) (data management is in the public interest or entrusted to the data controller

necessary for the execution of a task performed in the context of the exercise of public authority).

In rather exceptional cases, the data controller Article 6 (1) point a).

(contribution) can also be used as a legal basis.

In the case of point f) of Article 6 (1), video camera surveillance is legal, if it is

it is necessary to enforce the legitimate interests of the data controller or a third party, unless such is the case

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

rights and

freedoms. The legitimate interests of the controller or a third party may be legal, economic or otherwise

are of a financial nature. However, the data controller must take into account that if it is

the person concerned objects to the monitoring pursuant to Article 21, then the data controller only then

may continue to monitor the concerned video camera if there is a compelling legitimate interest to do so

justifies it, which takes precedence over the interests, rights and freedoms of the data subject,

or which is related to the presentation, enforcement or defense of legal claims.

If the data controller complies with Article 6 (1) point f) of the General Data Protection Regulation

you choose your data management

as its legal basis, it must carry out an interest assessment. This round it is

data controller must examine the necessity of data management. Handling of personal data

2 Access link for European Data Protection Board guideline No. 3/2019: 3/2019. guideline no. personal data

on handling with video devices | European Data Protection Board (europa.eu)

it must be directly related to the goal to be achieved: the goal is precise, complex and

must be examined with a fact-based analysis, particularly whether there is a less restrictive one

means to achieve the desired goal, are there other alternatives, the private sphere of the stakeholders less

restrictive devices. The legitimate interest of the data controller or the third party must be determined a

as precisely as possible, a fact-based, specific investigation of the given data manager

Based on. The interest must be real and current. It is a fundamental element of the consideration of interests

assessment of stakeholder interests and expectations, attention must be paid to the status of the stakeholders, legal and

their actual situation, as well as their reasonable expectations regarding data management. The

interest assessment is a detailed analysis of why the controller restricts proportionally

its legitimate interest, the rights of the data subjects, and why it follows from the revealed facts that it is in the interest of the

data controller

its primacy over the rights of those concerned. In the absence of such a consideration of interests, it is subject to consideration

to the detriment of the principle of accountability - there can be no question of legal and transparent data management. The

in the balance of interests, the person of the data controller and the data controller must be clearly defined

it is his responsibility and task to accurately document and justify the above. Legitimate interest is a legal basis

its existence must be based on a consideration of interests3

(47)

also based on its preamble. Article 5 (2) of the General Data Protection Regulation

based on the data controller must be able to prove that in the general data protection regulation

your data management complies with what was written, i.e. that you have carried out the interest assessment.

verify the general data protection

ordered

According to the constant and consistent practice of the Authority, the data controller is responsible for what he has done

for the legality of data management. Article 6 (1) point f) of the General Data Protection Regulation

due to the nature of the legal basis according to

the processing of specific personal data is based on the legitimate interest of the data controller, and on this

in view of the interest, why data management is necessary, you must also be able to verify and prove,

that priority is given to the legitimate interest of the data subject, related to the protection of personal data

against his right.

Based on the Applicant's request, the Authority established that in the present case, the Applicant

data management does not comply with the referenced legal provisions due to the following:

IV.2.1. Findings related to the legal basis

In this case, the legal basis for data management related to camera surveillance is the Respondent

according to his statement, according to Article 6 (1) point d) of the General Data Protection Regulation

protection of vital interests.

As stated in the Guidelines, the legal basis for camera surveillance is mostly applicable

the legitimate interest of the data controller or a third party in accordance with Article 6 (1) point f) of the GDPR

may be the legal basis for a vital interest according to Article 6 (1) point d) of the GDPR

Nor does the guideline list it among the legal bases that realistically arise, that – taking into account (46)

also for the preamble - it cannot be used with surveillance by the camera system

for related data management. On the one hand, the Authority points out that the Respondent did not prove that

data management would not be possible on any other legal basis, or the basis for point d) listed there

Public or private interests similar to reasons have not been identified by the Respondent in the present case, and

the Authority could not establish this either.

In view of the above, the Authority concludes that the Respondent by being on the terrace

the operated camera system continuously records images and sounds for those involved

uses personal data without legal basis.

3 The Data Protection Working Group 6/2014 provides assistance in carrying out the interest assessment. No. 95/46/EC, the

data controller

his opinion on the concept of his legitimate interests according to Article 7. The opinion is available from the following link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf

The Authority is for the part of the request relating to point d) of Article 58 (2) of the GDPR

examined whether the examined data management can be made legal.

The Authority emphasizes that there are only limited, express legal requirements for monitoring public areas

is possible, as this activity may offend the person observed by the camera

your privacy by processing your personal data even against your will.

Camera surveillance can be carried out in public areas primarily on the basis of legal authorization (e.g.:

police data controllers, Act XXXIV of 1994 on the Police. based on § 42 of the Act, a

public space supervision, LXIII of 1999 on public space supervision. Act 7-7/A. § -the

on the basis of the armed security guards, about the armed security guards, nature conservation and

CLIX of 1997 on field guard service. Act 9/A. based on §). Also exceptionally

surveillance based on legitimate interest is also conceivable to a necessary and proportionate extent, however

it is important that this does not allow everyone to demarcate their private property without limit

observe a public area with reference to the fact that an act may take place at any time, due to which

it may be necessary to record it, that is, each e.g. with authority for law enforcement duties and

competent authorities

his task should be taken over by persons who do not

have the appropriate authority.

owned by

Guidelines 3.1.2.

paragraph 27 of the chapter in addition to establishing that

The

camera designed to monitor the area

generally own

the application of an observation system can extend to the border of the area, also admits that it is exceptional

case, a situation may arise where the scope of camera surveillance cannot be narrowed down

within its own territory, since in this way it would not be sufficiently effective

protection. Adequate technical or organizational measures (for example, the purpose of the monitoring

covering an area that is not relevant from the point of view or the monitored part with IT tools

filtering), the data controller is entitled to extend camera surveillance

also to the immediate surroundings of the privately owned area.

At the same time, in the event that the data controller does not use public space masking

solutions, or who purposefully operates a camera system monitoring public areas,

must apply the general data protection regulation specified for data controllers

must base its data management on an appropriate legal basis, among other things.

Based on the camera images available to the Authority, it was established that the Applicant

cameras operated by monitor public space, but at the same time it was sent to the Authority

on the basis of a usage agreement, it can also be stated that the Respondent legally uses the

The public space at […] is a terrace catering to the area in front of and next to the store

for placement purposes.

The Authority also established, based on the viewing angles of the cameras and presentation snapshots,
that they do not observe the entrance to the residential building objected to by the Applicant, given that
that the viewing angle of the devices is directed towards public space, but they are directed by the Applicant
a terrace is observed. Photographs sent by the Applicant and the Respondent
and based on evidence, it was not proven that the Respondent changes the cameras
point of view in order for the Applicant to monitor the movement of the residents of the apartment building at […]
also under observation
to keep At the same time, it can be established that the Applicant
the entrance of his residential property directly next to the camera system operated by the Applicant
is located, so whoever wishes to approach the property inhabited by the Applicant from the direction of […]
entrance, the image of those persons to be recorded by the camera system operated by the Applicant
occurs without the Respondent changing the cameras' angle of view of the residents' movements
in order to observe.
Based on the Applicant's statement, the camera system was installed because a
on the terrace
I live
previously providing protection of stored assets
due to chain rattling a
you know
12
or directly a
prior to installation, a guest is violent
they complained
committed a crime against a person in the Respondent's sphere of interest.
In addition, the Respondent indicated that the installed camera system helped the police
his work,

given that another can be found directly next to the Applicant

in relation to a catering unit, theft of a small value by force against property

a crime was suspected, in connection with which it was operated by the Respondent

a video recording recorded with a camera system was seized by the police.

According to the Authority's findings - taking into account the attached police report concerning the neighboring business

documents, or the interests of the Applicant

committed against a person belonging to

for a crime - the legal basis of legitimate interest can also be used in certain circumstances,

however, for the legal application of this, the data controller must consider the data management

circumstances and to the data controller

to support the priority of its legitimate interest

must prepare a balance of interests test, especially given that the current statutory

provisions, or the principle of accountability, the data controller must certify

that the electronic monitoring system it uses is compatible with the purpose

bound by the principle of data management and the outcome of the interest assessment is the legitimate interest of the data

controller

resulted in its priority.

Regarding the legal basis of legitimate interest, the Guidelines emphasize that it poses a direct threat

situations, or in areas known as typical locations for crimes against property,

The purpose of protection against burglary, theft or vandalism in a real and dangerous situation is a

may be considered a legitimate interest in video surveillance. The European Data Protection

According to the board's position, it is recommended that data controllers record the previous illegality in writing

the relevant circumstances of the acts and the fact that a report was filed in the case. Likewise

the existence of a legitimate interest can also be proven if the data controller is a criminal in the given area

taking into account its statistics and the experiences of shops in the area, it comes to the conclusion that

that illegal acts can be expected in the given area.

In the case of camera surveillance systems, the Guidelines specify the necessity of

examines whether other types of security measures (e.g. fencing the property,

employment of security personnel) may provide equally effective protection where applicable

against burglary, theft and vandalism, such as the camera system.

In the event that the data controller wishes to prevent crimes against property,

instead of installing a video camera surveillance system, other types of security measures are also being implemented

can, for example, fence the property or assets to be protected, regular patrols

you can entrust the security staff with its performance, you can provide better lighting, security

you can install locks and burglar-proof doors and windows. These measures are equally effective

against theft and vandalism, like a video camera

can provide protection against burglary, a

monitoring systems. The data controller must assess on a case-by-case basis that such measures

whether they can be a reasonable solution.

Based on the Applicant's statement, prior to the installation of the camera surveillance system, a

previously used chain fencing to protect property on the terrace,

which, however – the residents with the noise associated with the chain rattling associated with this measure

due to their objections - terminated by the Respondent.

According to the Authority's point of view, if the Respondent had prepared an interest assessment

test, it is justified to demonstrate why the data management activity cannot be performed otherwise

method, such as the management of personal data. The General Data Protection Regulation (39)

according to the preamble, personal data can only be processed if it is

the purpose of data management cannot be reasonably achieved by other means.

The Authority also highlights point 38 of the Guidelines, according to which those concerned can expect,

not to be observed in public places, especially if these places

typically used for convalescence, relaxation and leisure activities, as well as

in places where individuals stay and communicate, such as lounges,

at restaurant tables, parks, movie theaters and fitness facilities. In this case it is

the interests or rights and freedoms of the data subject take precedence over the legitimate interests of the data controller

against.

The Authority determines that, based on point 38 of the Guidelines, the

its data management related to the camera surveillance system is disproportionate from the point of view,

that those concerned can expect not to be observed in public places of rest and

during their leisure activities, such as the Applicant's terrace. As a result, the

According to the authority's findings, the videotaping by the Respondent cannot be considered legal

data management with a monitoring system during opening hours, given that it is a restaurant

observes tables where, as appropriate, individuals pursue their leisure activities. THE

Based on the GDPR and the Guidelines, this data management does not comply with the principle of proportionality.

According to point 26 of the Guidelines, operating at night and outside normal working hours

monitoring system usually meets the data manager's needs for threats to his assets

to avoid Based on this, if it can be verified on the basis of other circumstances of data management a

necessity, then - taking into account e.g. to the size of the protected values - night and normal

monitoring system operating outside working hours for public areas

directing proportionate restriction

can implement. However, audio recording is not considered at night and outside normal working hours

according to the Authority's point of view, it is a legal method of data management.

The Authority emphasizes that the Applicant needs to present the

the need to use a monitoring system -

considering the usage

the authorization resulting from the agreement, the legal use of the area, as well as the fact that a

The applicant keeps assets of greater value in the monitored area - however, a

According to the authority's point of view, the legitimate interest exists at most at night and during normal working hours

can be accepted for an outside period.

At the same time, the Authority draws attention to the fact that, in view of the fact that previously

the application of the chain in order to achieve the Asset Protection goals of the Respondent has been proven, - it is

despite the objections expressed by some residents in connection with noise - since the chain a

a less privacy-infringing solution than with a camera

so the

The applicant must prove that, despite this, for what reason he still applies the

a solution that restricts the private sector more severely.

IV.3. Informing those concerned about camera surveillance

data management,

For data subjects in Article 13 (1) and (2) of the General Data Protection Regulation

in accordance with the provisions, it is necessary to provide information about the circumstances of data management.

Chapter 7 of the Guidelines provides detailed information for those concerned

in connection with information. According to this, in the case of camera surveillance, the data controller

a multi-level approach should be used and to ensure transparency a

regarding video camera surveillance, the most important information on the warning sign (first

level) must be indicated, and the additional mandatory data can be provided in another way (second level).

The first-level information (warning sign) must be displayed so that the affected person is the observed one

before entering the area, you can easily recognize the circumstances of the surveillance. Usually a

must contain the most important information, such as, for the purposes of data management, the data controller

detailed information on the identity and the rights of the data subject. They can belong here

for example, the legitimate interests of the controller (or third party) and (if applicable) data protection

official contact details. In addition, reference should be made to the more detailed, second-level information,

as well as the place and method of its availability. In addition, a pictogram can also be applied to it

in order to be clearly visible to those concerned with the camera surveillance system

data management.

The second level of information must also be in a place easily accessible to the person concerned

to be made available, for example in a central location (at the information desk, reception or

at the checkout) in the form of a comprehensive information sheet or easily visible poster.

In accordance with the above, the first level warning sign must clearly refer to the

for second level information. In addition, in the first level of information - if available

with this the data controller - it is worth referring to the digital source of the second level of information

(e.g. QR code or website address). However, the information is not in digital form either

should be made easily accessible. The second level of information is for the monitored area

without logging in

should also be available, especially if it is released digitally

available (this can be solved, for example, by specifying a link). It is provided in any form

the information, it must contain in accordance with Article 13 of the General Data Protection Regulation

all information required.

The Applicant has attached the photograph showing the pictogram pasted on the front door,

and the Respondent stated that in their drink labels with the same pictogram and

text also informs those concerned about the camera surveillance system, however

in addition, additional data management information can be found in Article 13 (1) and (2) of the General Data Protection

Regulation

in accordance with paragraph 1, the Respondent did not provide the affected parties, so the Authority

states that the Respondent has violated Article 13 (1) of the General Data Protection Regulation and

(2) paragraph.

IV.4. Request to delete personal data

The Applicant's request for the deletion of personal data managed by the Respondent is its own

was interpreted by the Authority to delete his personal data, given that the Applicant thereby

in this context, you can only submit a request for this purpose. At the same time, because he did not stand

at the disposal of the Authority, evidence indicating that the Respondent is a replica of the Applicant

would have managed during the period under review, therefore the Authority rejected this part of the application.

IV.5. Legal consequences

Pursuant to the above, the Authority is Article 58(2)(b) of the General Data Protection Regulation

was condemned by the Respondent, as its data management activities violated the general

the provisions of the data protection decree, and pursuant to point d) of the same paragraph, the Authority

obliged the Applicant to perform its data management operations - as appropriate, in a specified manner

and defined

within a period of time - harmonized by the general data protection regulation

with its provisions as indicated in the relevant section.

The Authority ex officio examined whether a data protection fine against the Application was justified

imposition. In this context, the Authority has Article 83 (2) of the GDPR and Infotv.75/A. on the basis of §

ex officio considered all the circumstances of the case and found that during the present proceedings

in the case of a detected violation, the imposition of a fine is neither proportionate nor necessary, given that

that the Respondent has not previously established a violation of the GDPR. THE

According to the Authority's point of view, the Applicant can be reached without imposing a data protection fine

demand that the Respondent, as a data controller in the future, GDPR

perform data management in accordance with its rules.

Based on the above, the Authority decided in accordance with the provisions of the statutory part.

15

A. Other questions

The competence of the Authority is set by Infotv. Paragraphs (2) and (2a) of § 38 define it, and its competence is

covers the entire territory of the country.

The decision is in Art. 80-81 § and Infotv. It is based on paragraph (1) of § 61. The decision is in Art. 82.

Based on paragraph (1) of § §, it becomes final upon its communication. The Akr. § 112 and § 116, paragraph (1),

and based on § 114, paragraph (1), the decision can be challenged through an administrative lawsuit

as a remedy.

* * *

The rules of the administrative trial are set out in Act I of 2017 on the Administrative Procedure

hereinafter: Kp.) is defined. The Kp. Based on § 12, paragraph (1), by decision of the Authority

the administrative lawsuit against falls within the jurisdiction of the court, the lawsuit is referred to in the Kp. § 13, subsection

(3) a)

Based on point aa), the Metropolitan Court is exclusively competent. The Kp. Section 27 (1)

legal representation is mandatory in a lawsuit falling under the jurisdiction of the court based on paragraph b).

The Kp. According to paragraph (6) of § 39, the submission of a claim is an administrative act

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

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

CCXXII of 2015 on the general rules of administration and trust services. law (a

hereinafter: E-administration act) according to § 9, paragraph (1), point b) of the customer's legal representative

obliged to maintain electronic contact.

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

information about a simplified trial in Kp. Paragraphs (1)-(2) of Section 77 and Paragraph (1) of Section 124

and (2) point c) and (5) respectively. The fee for the administrative lawsuit

XCIII of 1990 on fees. Act (hereinafter: Itv.) 45/A. (1) of §

Define. Regarding the advance payment of the fee, the Itv. Section 59(1) and Section 62(1)

paragraph h) exempts the party initiating the procedure.

If the Respondent does not adequately certify the fulfillment of the prescribed obligation, the Authority

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

the obligee has not complied with the obligation contained in the final decision of the authority, it can be enforced.

The Authority's decision in Art. According to § 82, paragraph (1), it becomes final with the communication. The Akr.

The Akr. Pursuant to § 133, enforcement - unless otherwise provided by law or government decree

has - it is ordered by the decision-making authority. The Akr. Pursuant to § 134, the execution - if

law, government decree or, in the case of municipal authority, a local government decree

does not provide otherwise - it is undertaken by the state tax authority. Infotv. § 60, paragraph (7).

on the basis of the Authority's decision to carry out a specific act, specified

the decision regarding the obligation to conduct, tolerate or stop

its implementation is undertaken by the Authority.

dated: Budapest, according to the electronic signature

Dr. Attila Péterfalvi

president

c. professor