

Case number: NAIH-308-5/2022.

(NAIH-6457/2021.)

Subject: infringement notice and request

partially rejecting decision

H A T A R O Z A T

The National Data Protection and Freedom of Information Authority (hereinafter: Authority) is [...]

(residential address: [...]; hereinafter: [...]) acting in its legal representation [...] ([...] Lawyer; registered office:

[...]; KASZ: [...]) to the Authority's request on August 3, 2021, the request

with cameras operated by [...] (residential address: [...]; hereinafter: Applicant).

in a data protection official proceeding concerning related data management - in which the

Authority also granted customer legal status to [Customer] (address: [...]) - the following decisions

brings:

1. The Authority grants the Applicant's request in part and condemns the Applicant

and [the Customer] because the processing of personal data of natural persons

regarding its protection and the free flow of such data, as well as 95/46/EC

Regulation (EU) 2016/679 on the repeal of the directive (hereinafter: general

data protection decree) in violation of Article 6 (1) and without a legal basis

data management in connection with their cameras No. 4 and 5, with the fact that they allow the Applicant,

respectively, their property is monitored.

2. The Authority rejects the request concerning cameras No. 1 and 2 monitoring the public area

part, but at the same time ex officio condemns the Applicant and [the Client] because it is

violate Article 6 (1) of the General Data Protection Regulation and continue without a legal basis

data management in connection with their cameras No. 1 and 2, with the fact that they a

public space and the persons concerned staying there are observed.

3. At the request of the Applicant, the Authority instructs the Applicant and [the Client] that the

terminate the illegality within 30 days from the date of this decision becoming final

data management, they bring their data management operations into line with the legal provisions  
by that

- modify the angle of view of cameras No. 4 and 5 so that they are not directed to

On the applicant's property, or

- apply a masking function using software that provides masking

when making recordings, or

- mechanically cover the area of the Applicant's property Nos. 4 and 5

from the point of view of cameras, or

- remove cameras 4 and 5.

4. At the request of the Applicant, the Authority instructs the Applicant and [the Client] that the  
Nos. 4 and 5 shall be deleted within 30 days from the date of the finalization of this decision  
illegal recordings recorded by cameras.

5. The Authority ex officio instructs the Applicant and [the Client] that the present  
terminate the illegal within 30 days of the decision becoming final

.....  
.....

1055 Budapest  
  
Falk Miksa utca 9-11  
  
Phone: +36 1 391-1400  
  
Fax: +36 1 391-1410  
  
ugyfelszolgalat@naih.hu  
  
www.naih.hu

2  
  
data management, they bring their data management operations into line with the legal provisions  
by that  
  
- modify the viewing angle of cameras No. 1 and 2 so that they are not directed

public space, or

- apply a masking function using software that provides masking

when making recordings, or

- the public area is mechanically covered from the view point of cameras No. 1 and 2,

obsession

- remove cameras 1 and 2.

6. The Authority ex officio instructs the Applicant and [the Client] that the present

Cameras No. 1 and 2 should be deleted within 30 days of the decision becoming final

illegal recordings recorded by

7. The Authority ex officio condemns the Applicant and [the Client] for not

provided adequate information about their data management related to camera surveillance,

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

8. The Authority ex officio instructs the Applicant and [the Client] that this decision

13 of the General Data Protection Regulation 30 days after it becomes final.

information on data management in accordance with paragraphs (1)-(2) of Article

9. The Authority rejects the Applicant's request for the imposition of a data protection fine

part.

Taking the measures prescribed in points 3, 4, 5, 6 and 8 to the Applicant and [the

Customer] must in writing within 15 days of taking the measure - that

together with the submission of supporting evidence - to prove it to the Authority. The 3rd, 4th, 5th, 6th

and in case of non-fulfillment of the obligation according to point 8, 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 claim must be submitted to the Authority electronically, 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. Those who do not benefit from the full personal tax exemption the fee for the judicial review procedure is HUF 30,000, the right to note the fee subject to the lawsuit falls below Legal representation is mandatory in proceedings before the Metropolitan Court.

## I N D O C O L A S

### I. The sales process

On August 3, 2021, the Applicant's request for initiation of official data protection proceedings appealed to the Authority, as he complained that it was installed by the Respondent surveillance cameras do not only record data on your own property, but also on the Applicant's both on property and on public land. According to the Applicant, also according to the Respondent's own declaration The cameras are located three hundred meters away in public areas.

The Applicant requested in his application that the Authority Article 58 of the General Data Protection Regulation Based on points f), g) and i) of paragraph (2), oblige the Applicant to use the cameras

3

remove it, delete the data stored about the Applicant and his property, and the Authority out administrative fine.

### I I . Cleaning up the reality

1. In order to clarify the facts in the official data protection procedure, the Authority requested the 2021. dated August 11, NAIH-6457-2/2021. to make a statement in the order with file number called the Applicant. The Authority's order was returned to the Authority by the Respondent according to the receipt, he received it on August 16, 2021, to which the Applicant also responded with an email dated August 16, 2021.

In this letter, the Respondent described that he had installed four cameras on his own property due to his observation because several of his purebred dogs were poisoned while in front of his house his parked vehicle was vandalized by school children. The cameras are in your own yard, outside parked car and the gate of his mother-in-law who lives next door. The Applicant to support this, he sent screenshots confirming the viewing angles of the cameras.

According to the Respondent's statement, the analog cameras have Internet access, which serves to take into account that the Respondent's mother is disabled, who is alone you are in your home, if you hear a dog barking or a noise, you can see the moment picture and can notify the Applicant if there is any problem.

According to the Applicant's statement, the cameras record movement, and their storage time is 3 days corresponds to. According to the Applicant's statement, he uses the recordings for the above purposes, does not forward them to anyone, and does not record any recordings of the applicant, and he doesn't use it, because the camera doesn't even take him.

Furthermore, according to the Respondent's statement, the cameras do not record sound, because they are not suitable for that.

According to the Respondent's statement, he verbally informed the Applicant that cameras were installed due to vandalism and animal poisoning, who was even happy that his new fence, if someone vandalized it, he could look at it, however, the Respondent informed him that a camera only sees in front of his gate.

The Authority dated 30 August 2021, NAIH-6457-4/2021. with order no called the Applicant, either by post or in person, or - if it is voluntarily undertook electronic administration - in possession of a customer portal on the e-Papír service submit your declaration through, bearing in mind that the general administrative CL of 2016 on public order. Act (hereinafter: Act) and electronic administration and CCXXII of 2015 on the general rules of trust services. law (a hereinafter: Eüsztv.) to the Respondent in order to be legally binding be able to make a statement, in writing, by electronic means specified in the Eüsztv. - in possession of the customer portal via the e-Paper service - or in person, in writing must keep in contact with the Authority through non-qualifying electronic means, which is also appropriate from Akr., as well as identification and electronic identification resulting from the Eüsztv

obligation. Given that the statement came in the form of a simple email

not suitable for identification, does not qualify as defined in the Ákr. or the Eüsztv.

method of contact, so it is not suitable for triggering legal effects.

The Applicant is Authority NAIH-6457-4/2021. case file number is also simple e-

replied in the form of an email. In his reply, he stated that if he could,

would personally comment on the matter, but he lives in [...], does not have a customer portal, and

4

he works from Monday to Friday, so he cannot comply with the requirements of the Authority's order. On this

besides, his wife is physically disabled, so she cannot contribute to the mailing of the letter either. [...].

In view of this, the Authority dated September 15, 2021, NAIH-6457-6/2021.

in his order with case file number, he repeatedly called on the Applicant that in the Ákr.

Submit your statement in accordance with the contact method specified in Eüsztv.

The Authority NAIH-6457-6/2021. on September 22, 2021, for the order with file number a

Instead of being requested, [the Customer] made a statement through the customer portal. His statement is verbatim agreed with the statement made by the Respondent in an e-mail, as well as [the Customer].

sent screenshots verifying camera angles. At the same time, the Applicant a

Authority NAIH-6457-6/2021. he did not make a statement for the order with case file number.

In view of the above, the Authority dated September 29, 2021, NAIH-6457-8/2021.

in his order with file number, he informed [the Client] that since the case, his right, is legitimate

interests are directly affected, therefore the Authority in the procedure referred to in Art. to paragraph (1) of § 10

granted him the legal status of a client, and in order to clarify the facts

to make a statement, or, if acting as a representative of the Respondent, representative

called him to prove his right.

The Authority NAIH-6457-8/2021. He responded to his order with file number on October 4, 2021 [i.e

Customer], in which he stated, among other things, that he installed and operates the cameras.

He also attached to his letter his power of attorney authorizing him to represent the Respondent. [The

Customer], however, did not send it in addition to the authorization presented by the Respondent statements, and the Respondent did not respond. [The Customer's] reply letter attachment at the same time, it was formed by a floor plan made of a property, according to which it is on the property of the Applicant – [...] – cameras are in operation.

The Authority dated 11 October 2021, NAIH-6457-14/2021. in the order with file no to the question, [the Customer] stated in his letter dated October 14, 2021 that on the one hand, he is making a statement, and on the other hand, he is also acting on behalf of the Respondent, who has done so before reserves its statements.

In addition, [the Client] stated that he discussed the installation of the cameras with his husband, a They decided jointly with a request, about 4 years since he became disabled and he is alone at home, often at night. According to his statement, there were several burglaries in the village and then more their purebred dog was poisoned, while a large amount of damage was done to the car parked in front of the house kids. That is why they decided to install the cameras, which were installed by his son.

According to [the Customer]'s statement, he operates the cameras and can open one from a phone With an app called Hik-Connect. He doesn't watch it day and night, but only when he hears a big noise opens the application in which you see the snapshots. This is [the Client] and his family also reassures him, because if there is a problem, he will be able to notify them.

According to [the Customer]'s statement, the purpose of operating the cameras is only for its own values and protecting your safety. The cameras - which, according to the statement, are not surveillance cameras - they look at your own yard, garden and the gate of the house, not the neighbor.

2. Furthermore, considering that the Applicant's legal representative did during the procedure according to his statement, the Respondent operates not four, but five cameras, the Authority does Article 58 (1) point e) of the General Data Protection Regulation, as well as the information CXII of 2011 on the right to self-determination and freedom of information. law (a hereinafter: Infotv.) based on Section 71 (1b) he contacted the Clerk of [...] Municipality

(hereinafter: notary) to check the Applicant or [the Client] at [...]

5

the conditions of data management carried out by and provide information requested by the Authority regarding data management issues.

The minutes of the on-site inspection sent by the notary - and the one attached to it, screenshots showing the angle of view of the cameras - according to four at the time of the on-site inspection one camera was operating in the area of the property at [...], and one was not working. THE camera type: Hikvision DS-2CE16DOT-IT3F 2.8mm, IP cameras, with internet access. THE according to the protocol, the viewing angles of the cameras to the property owner's private area are directed. The cameras record footage, but there are no computers or monitors connected to it, and they only record images, not sound. Note that the cameras are not connected to a computer, log files were not viewed.

According to the protocol, for the live image transmitted by the cameras, as well as the recorded and stored the user, [the Customer], has access to recordings via the Internet mobile application - Hikvision version: V4.16.04.0706 - you can use the recordings watch.

3. Regarding the fifth camera objected to by the Applicant's legal representative, [the Client] stated, that it only sees momentary images, but it is broken, but at the same time, according to his point of view, neither is it overlooks the Applicant's yard. He sent an old picture to support this.

4. Based on all this, it can be established that the Respondent and [the Customer] five cameras operates. The one sent by them and the clerk, showing the angle of view of the cameras based on screenshots, it can also be established that two of the five cameras – 1. and camera number 2 - its angle of view also overlooks the public area in front of the house, while two cameras - 4 and 5 camera number - to the Applicant's property and yard. A camera, number 3 is which does not see beyond the property of the Respondent and [the Client].

III . APPLICABLE LAW REGULATIONS



According to the present case, based on Article 2 (1) of the General Data Protection Regulation the general data protection regulation shall be applied to data management.

Infotv. Pursuant to § 2, paragraph (2), the general data protection regulation is indicated there shall be applied with additions contained in provisions.

Infotv. According to § 60, paragraph (1), the right to the protection of personal data in order to enforce it, the Authority will initiate a data protection official procedure for this request initiates and may initiate official data protection proceedings ex officio. For the official data protection procedure the Akr. rules shall be applied with the additions specified in Infotv. and with deviations according to the general data protection regulation.

Infotv. Based on § 60, paragraph (2): "Regarding the initiation of the official data protection procedure request in Article 77 (1) of the General Data Protection Regulation, as well as Article 22 b) can be submitted in the case specified in

Pursuant to Article 77 (1) of the General Data Protection Regulation: "Other without prejudice to administrative or judicial remedies, all stakeholders are entitled to file a complaint with a supervisory authority – in particular your habitual residence, a workplace or in the Member State where the alleged violation occurred - if the person concerned in his opinion, the processing of his personal data violates this regulation."

According to Article 4, point 1 of the General Data Protection Regulation: ""personal data": identified or any information relating to an identifiable natural person ("data subject");

6

the natural person who, directly or indirectly, in particular, can be identified an identifier such as name, number, location data, online identifier or a physical, physiological, genetic, intellectual, economic, cultural or social natural person can be identified based on one or more factors relating to its identity."

Based on Article 4, Point 2 of the General Data Protection Regulation: ""data management": the personal conducted on data or data files in an automated or non-automated manner

any operation or set of operations, such as collecting, recording, organizing, categorizing, storage, transformation or change, query, insight, use, communication through transmission, distribution or otherwise making it available, coordination or linking, restriction, deletion or destruction."

Pursuant to Article 4, point 7 of the General Data Protection Regulation: "'data controller': the a natural or legal person, public authority, agency or any other body, which is 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 manager or the special aspects regarding the designation of the data manager it can also be determined by EU or member state law."

According to Article 26 (1) of the General Data Protection Regulation: "If the purposes of data management and its tools are defined jointly by two or more data controllers, they are joint data controllers qualify. The joint data controllers transparently, in the agreement between them shall be determined for the fulfillment of the obligations under this regulation, in particular the exercising its rights and providing the information referred to in Articles 13 and 14 the distribution of their responsibilities related to their duties related to the discharge, except that case and to the extent that, if and to the extent, the distribution of responsibility for data controllers determined by EU or Member State law applicable to them. It's in the agreement a contact person can be appointed for those concerned."

Based on Article 2 (2) point c) of the General Data Protection Regulation: "This regulation does not applies to the processing of personal data if:  
c) natural persons only in the context of their personal or home activities are carried out."

Pursuant to Article 5 of the General Data Protection Regulation: "(1) Personal data:  
a) must be handled legally and fairly, as well as in a transparent manner for the data subject conduct ("lawfulness, due process and transparency");

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

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

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

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

further data processing ("target binding");

c) they must be appropriate and relevant for the purposes of data management, and a

they must be limited to what is necessary ("data sparing");

d) they must be accurate and, if necessary, up-to-date; all reasonable measures

must be done in order to ensure that it is inaccurate in terms of the purposes of data management

have personal data promptly deleted or corrected ("accuracy");

e) must be stored in a form that allows the identification of the data subjects only a

enables the processing of personal data for the time necessary to achieve its goals; the

Personal data may only be stored for a longer period of time if

insofar as the processing of personal data is in accordance with Article 89 (1).

for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes

will take place for the purpose of protecting the rights and freedoms of those affected in this regulation

for the implementation of appropriate technical and organizational measures

subject to ("limited shelf life");

7

f) must be handled in such a way that appropriate technical or organizational measures

adequate security of personal data should be ensured by using

unauthorized or illegal handling, accidental loss or destruction

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

(2) The data controller is responsible for compliance with paragraph (1), and must also be able to

to demonstrate this compliance ("accountability")."

According to Article 6 (1) of the General Data Protection Regulation: "Personal data

its handling is legal only if and to the extent that it is 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 to which the data subject is a party party, or the steps taken at the request of the data subject prior to the conclusion of the contract necessary to do;

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 the data controller is authorized by a public authority necessary for the execution of a task performed in the context of its exercise;

f) data management to enforce the legitimate interests of the data controller or a third party necessary, unless the interests of the person concerned take precedence over these interests interests or fundamental rights and freedoms that make personal data protection necessary, especially if a child is involved.

Point f) of the first subparagraph does not apply to the performance of their duties by public authorities for data management during

Based on Article 13 (1)-(2) of the General Data Protection Regulation: "(1) If the data subject relevant personal data are collected from the data subject, the data controller is the personal data provides the following information to the data subject at the time of its acquisition all of them:

a) the identity of the data controller and - if any - the data controller's representative and your contact details;

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 appropriate, recipients of personal data, or categories of recipients, if any;

f) where appropriate, the fact that the data controller is in a third country or international organization wishes to forward the personal data to, and the Commission the existence or absence of its conformity decision, or in Article 46, Article 47 or in the case of data transfer referred to in the second subparagraph of Article 49 (1) a indicating appropriate and suitable guarantees, as well as obtaining a copy of them reference to the means or their availability.

(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 be fair and transparent provides data management, 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 it can object against the processing of such personal data, as well as the data subject about your right to data portability;

c) based on point a) of Article 6 (1) or point a) of Article 9 (2) in the case of data processing, the right to withdraw consent at any time,

8

and what it's like

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

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

e) about the provision of personal data

statutory or contractual

whether it is based on an obligation or a prerequisite for the conclusion of a contract, as well as whether the person concerned

are you obliged to provide personal data,

possible

failure to provide data may have consequences;

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

what are the expected consequences for the person concerned."

Pursuant to Article 58 (2) of the General Data Protection Regulation: "The supervisory authority

acting in its corrective capacity:

a) warns the data manager or the data processor that some planned data processing

its activities are likely to violate the provisions of this regulation;

b) condemns the data manager or the data processor if its data management activities

violated the provisions of this regulation;

c) instructs the data manager or the data processor to comply with this regulation for the data subject

your request to exercise your rights under;

d) instructs the data manager or the data processor that its data management operations - given

in a specified manner and within a specified period of time - harmonises this regulation

with its provisions;

e) instructs the data controller to inform the data subject about the data protection incident;

f) temporarily or permanently restricts data management, including data management

also its prohibition;

g) in accordance with the provisions of Articles 16, 17 and 18, orders personal data

rectification or deletion, or restriction of data processing, as well as Article 17 (2)

and in accordance with Article 19, orders the notification of those recipients,

with whom or to which the personal data was disclosed;

h) revokes the certificate or instructs the certification body to comply with Articles 42 and 43

to withdraw a duly issued certificate or instruct the certification body to

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

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

depending, in addition to or instead of the measures mentioned in this paragraph; and

j) orders directed to a recipient in a third country or an international organization

suspension of data flow."

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

(2) The administrative fines, depending on the circumstances of the given case, are subject to Article 58 (2)

must be imposed in addition to or instead of the measures mentioned in points a)-h) and j) of paragraph

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

sufficiently in each case when determining the amount of the administrative fine

the following should be taken into account:

a) the nature, severity and duration of the infringement, taking into account the data management in question

its nature, scope or purpose, as well as the number of persons affected by the infringement, as well as

the extent of the harm they have suffered;

b) the intentional or negligent nature of the infringement;

c) damage suffered by data subjects on the part of the data controller or data processor

any measures taken to mitigate;

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

technical and organizational measures taken on the basis of Articles 25 and 32;

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

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

extent of cooperation to mitigate its effects;

g) categories of personal data affected by the infringement;

h) the manner in which the supervisory authority became aware of the violation, 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 manager or the data processor has complied with Article 40 to approved codes of conduct or approved certification under Article 42 for mechanisms; as well as

k) other aggravating or mitigating factors relevant to the circumstances of the case, for example, financial gain as a direct or indirect consequence of the infringement or avoided loss.

[...]

(5) Violation of the following provisions - in accordance with paragraph (2) - at most 20

with an administrative fine of EUR 000,000 or, in the case of businesses, the previous one

shall be subject to an amount of no more than 4% of the total annual world market turnover of a financial year, by imposing the higher of the two amounts:

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;

c) personal data for a recipient in a third country or an international organization 44–49. in accordance with Article;

d) IX. obligations according to the law of the Member States adopted on the basis of chapter;

e) the instruction of the supervisory authority according to Article 58 (2), and data management



temporary or permanent restriction or suspension of data flow

failure to comply with its notice or access in violation of Article 58 (1).

failure to provide insurance."

Infotv. Based on Section 71 (1b): "At the request of the Authority, the settlement

the clerk of the municipality checks the activities carried out in the area of competence by the Authority

the actual circumstances of data management indicated in the request, so in particular the processed

scope of personal data, operations performed with personal data and these operations

tools, as well as the technical and organizational measures applied by the data controller."

Infotv. 75/A. pursuant to § 83 (2)-(6) of the General Data Protection Regulation, the Authority

exercises its powers in accordance with the principle of proportionality,

especially with the fact that you are in the legislation regarding the handling of personal data

The regulations defined in the mandatory legal act of the European Union are being implemented for the first time

in the event of a violation, to remedy the violation - 58 of the General Data Protection Regulation.

in accordance with Article - primarily with the warning of the data manager or data processor

takes action."

10

I V Decision making

IV.1. The person of the data controller

According to Article 4, point 7 of the General Data Protection Regulation, it is natural or legal

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

together with others it determines [...]. However, the General Data Protection Regulation recognizes the

the concept of joint data controllers, which based on Article 26 of the General Data Protection Regulation then

occurs when the purpose and means of data management are shared by two or more data controllers

Define. Based on the facts revealed in this case about data management, the cameras

about the equipment and the purpose of operating the cameras, the Applicant and [the Client]

decided jointly, so they are joint data controllers in terms of camera data management

qualify.

## IV.2. Legality of camera data management

### IV.2.1. Separation of household and non-household data management

Based on Article 4, Point 1 of the General Data Protection Regulation, the image of the data subject is personal is considered data. The identified or identifiable natural person is affected. All of these pursuant to, if a natural person can be identified based on a recording, then the taken image is personal data, the taking of the image is data management it counts as.

The application of the camera may be suitable based on its placement and angle of view to observe other private areas or public areas, for other properties make related recordings, which may offend the persons observed with the camera personal rights and privacy.

Based on point c) of Article 2 (2) of the General Data Protection Regulation, they do not belong to regulation, so the rules of the general data protection regulation do not have to be applied for the processing of personal data, if it is exclusively personal or natural persons home (so-called private or household

data handling). The general data protection regulation applies to personal or home activities

Recital (18) provides examples, so correspondence is classified as such, a address storage, carried out in the context of personal and home activities, on social networks contact and other online activities. However, it is important to point out that – as established by the Court of Justice of the European Union in the so-called Rynes judgment<sup>1</sup> - a the exception rule for private data management must be interpreted narrowly. On this according to the decision, the camera surveillance - in that part, if it is it also covers persons staying in an area outside the private property of the data controller - no falls under the said exception.

This practice was maintained by the European Data Protection Board<sup>2</sup> for personal data

with video devices

(the

3/2019 on the management of no

are carried out as part of their activities

in its guidelines

1 C 212/13. case number is available from the following link:

<http://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=HU>

2 The European Data Protection Board deals with issues related to data protection and the protection of privacy,

independent European advisory body.

11

guideline)<sup>3</sup>. The

and at home"

guidance in addition to establishing that

in the following:

in general, a camera set up for the purpose of monitoring one's own territory

the application of the monitoring system may extend to the border of the area, he admits that in exceptional cases

a situation may arise where the scope of camera surveillance cannot be narrowed down to your own

within the property area, as in this way it would not provide 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 is IT

filtering with devices) in addition to applying, the individual is entitled to extend the

camera monitoring of the immediate surroundings of the property.

At the same time, in the event that the private individual does not use the public space or the

solutions covering other private areas in the field of view of the camera, or who purposefully a

operates a camera system monitoring public areas or other private areas, already

becomes a data controller, and its activity is not classified as private data processing, thus therefore, the provisions of the General Data Protection Regulation for data controllers must be applied all regulations. Masking can therefore be used to narrow down what is observed by the camera area to the area owned by the data controller. However, if the cameras angle of view of the private sphere of the person handling data with the camera surveillance system to the outside - for example, to a public area, to an area jointly owned by a condominium, or other to an area owned by a third party - it is not considered subject to the above exception belonging to "personal, activity. For this reason, the given data management activity falls under the scope of the general data protection regulation, which thus - among others between - the basic principles according to Article 5 of the General Data Protection Regulation must apply, and for which the appropriate legal basis according to Article 6 of the General Data Protection Regulation required.

In this case, the Respondent and [the Client] operate five cameras. By them as well as based on the screenshots sent by the clerk showing the angle of view of the cameras it can also be established that two of the five cameras - cameras No. 1 and 2 - have a its angle of view also overlooks the public area in front of the house, while two cameras – cameras no. 4 and 5 – have For the applicant's property and yard. One camera, number 3, is that of the Respondent and does not see beyond [the Customer's] property.

#### IV.2.2. Cameras monitoring the Applicant and his property

Based on the above, it can be concluded that three cameras - cameras no. 4 and 5 - a its angle of view overlooks the Applicant's property and yard.

Consequently, it can be established that the viewing angle of the 4th and 5th cameras is the Requested and outside [the Client's] private sphere, owned by another third party, i.e. the Applicant is also aimed at stationary areas, therefore the data management cannot be considered as data management for private purposes.

For this reason, the data management activity related to camera surveillance in the present case is falls under the scope of the General Data Protection Regulation, to which, among other things, the basic principles according to Article 5 of the General Data Protection Regulation must apply, and which requires a suitable legal basis according to Article 6 of the General Data Protection Regulation. Although in order to achieve the property and life protection goals indicated by the Applicant and [the Client] cameras on their property may be potentially suitable, however a

The monitoring of the applicant, realized in this way, is permanent, without restriction for everyone extensive data management cannot be proportionate to the protection of the Applicant's personal data 3 of 3/2019. guideline no. is available from the following link:

[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_201903\\_video\\_devices\\_hu.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_hu.pdf) (chapter 3.1.2, point 27)

12

with its related interest. In this way, the Applicant and [the Client] to the Applicant and its property violated Article 6 of the General Data Protection Regulation with his observation, as a The applicant's personal data were and are being managed without an appropriate legal basis.

#### IV.2.3. Cameras monitoring public space

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

Among the cameras requested and operated by [the Customer], cameras No. 1 and 2 are the it also observes the area beyond the line of the fence that marks the plot boundary, i.e. public land.

Based on Article 77 (1) of the General Data Protection Regulation, all data subjects are entitled to file a complaint with a supervisory authority, in Hungary the Authority, if any according to the opinion of the data subject, the processing of personal data concerning him violates the general data protection regulation.

In this case, the Applicant did not prove that the Applicant and [the Customer] operated

Cameras 1 and 2 would have recorded him as the person involved. In the absence of involvement, the Authority an application for the official data protection procedure cannot be submitted, or the objected to in relation to data management, according to the provisions of the General Data Protection Regulation

to check compliance - upon request - the Authority does not have the right to this data protection within the framework of an official procedure. The Authority therefore rejects the Applicant's request in this a part.

At the same time, given that the operation of the cameras monitoring the public area is closely is related to the data management objected to by the Applicant, the Authority investigated it ex officio the legality of data processing with cameras.

Public space can only be monitored in a narrow circle, according to express legal regulations possibility, as this activity may violate the privacy of the person observed by the camera by processing your personal data even against your will.

IV.2.1. mentioned in point 3/2019 issued by the European Data Protection Board guideline 3.1.2.

paragraph 27 of the chapter in addition to establishing that

in general, a camera set up for the purpose of monitoring one's own territory

the application of the monitoring system may extend to the border of the area, he admits that in exceptional cases a situation may arise where the scope of camera surveillance cannot be narrowed down to your own within the property area, as in this way it would not provide 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 is IT devices), the data controller is entitled to extend the camera monitoring of the immediate surroundings of the property.

At the same time, in the event that the data controller does not use a public area cover 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.

To achieve the property and life protection goals indicated by the Applicant and [the Client].

these cameras may also be potentially suitable, however, passing through public areas,

and the monitoring of persons staying there - just as the Applicant and his property are monitored cameras as well – the constant, unlimited access to everyone realized in this way data management also cannot be proportionate to the field of view of the cameras present in the public area with the interest of protecting the personal data of the entering data subjects. In this way, the The Respondent and [the Client] also violated the general rules by monitoring the public area

13

Article 6 of the data protection decree, because the data subjects staying in public areas are personal your data has been or is being managed without an adequate legal basis.

#### IV.3. Information on data management

The Applicant's request did not cover information on data management, however, a The authority examined it ex officio as an obligation closely related to data management fulfillment. In order for the data management to be legal, it is an essential condition that the data controller must provide appropriate information about it. The relevant rules are is included in Article 13 (1)-(2) of the General Data Protection Regulation.

As part of the preliminary information, the data controller must strive to ensure that the data subject get as complete and comprehensive a picture of the handling of your personal data as possible, as the data subject this is the only way to assess the impact of a specific data processing on to his private sphere. Paragraphs (1)-(2) of Article 13 of the General Data Protection Regulation provide that contain the minimum data management conditions that data controllers need to inform the data subjects, but this does not mean that the controller is the data controller provide more precise information.

In the case of camera surveillance, preliminary information is already provided to the observed as a first step must be provided when entering the area. At that time, outside the observed area (entrance short information provided by means of a pictogram placed on the door, gate) is required, and at the same time is sufficient, which, at the same time, must be supplemented as a second step at least a full (longer and detailed) information sheet available on site.

The first brief information, i.e. the pictogram, usually contains the most important information must contain information about data management, such as the purposes of data management and the identity of the data controller and detailed information on the rights of the data subject. In addition, reference should be made to for more detailed, second-level information, as well as its availability location and way.

Information on the availability of this latter information must therefore be provided on the posted "pictogram".

(one of its functions is actually just this: it cannot be avoided when entering the area

for data management

if possible,

refers to its accessibility), and this information must be available at the request of the data subject

to forgive. The second level of information must already include general data protection

According to Article 13 (1)-(2) of the Decree, all mandatory data management requirements

information.

In the present case, the clerk attached the photograph showing the exterior wall of the front of the house

a stuck-on pictogram is visible, however, on the one hand, this did not include data management

relevant information, on the other hand, additional, second-level data management

no information was prepared. The Respondent and [the Client] thus did not provide the general

data protection

information is

about data management. The Authority therefore concludes that the Respondent and [the Client] have violated it

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

Sun. Legal actions

1. Based on Article 58 (2) point b) of the General Data Protection Regulation, the Authority a

Grants the Applicant's request in part and condemns the Applicant and [the Client]

because in violation of Article 6 (1) of the General Data Protection Regulation, legal basis



Compliant with paragraphs (1)-(2).

warns and the necessary

Regulation Article 13

information

comprehensive

14

without continuing data management in connection with their cameras No. 4 and 5, with the fact that they observe the Applicant and his property.

2. The Authority rejects the request concerning cameras No. 1 and 2 monitoring the public area

part, at the same time based on Article 58 (2) point b) of the General Data Protection Regulation

ex officio condemns the Applicant and [the Client] because of general data protection

In violation of Article 6 (1) of the Decree, data processing is carried out without a legal basis in accordance with Articles 1 and

2.

in connection with their camera number, with the fact that they are in the public area and the person staying there those involved are observed.

3. The Authority based on points d) and f) of Article 58 (2) of the General Data Protection Regulation

at the request of the Applicant instructs the Applicant and [the Client] that this decision

terminate the illegal data processing within 30 days of its becoming final,

bring their data management operations into line with legal provisions by

- modify the viewing angle of cameras No. 4 and 5 so that they are not directed to the

On the applicant's property, or

- apply a masking function using software that provides masking

when making recordings, or

- mechanically cover the area of the Applicant's property Nos. 4 and 5

from the point of view of cameras, or

- remove cameras 4 and 5.

4. Based on Article 58 (2) point g) of the general data protection regulation, the Authority a

At the request of the Applicant, he instructs the Applicant and [the Client] that this decision

be deleted by cameras No. 4 and 5 within 30 days of its becoming final

recorded, illegal recordings.

5. The Authority based on points d) and f) of Article 58 (2) of the General Data Protection Regulation

ex officio instructs the Applicant and [the Client] to make this decision final

terminate the illegal data processing within 30 days of the divorce

bring their operations into line with legal provisions by

- modify the viewing angle of cameras No. 1 and 2 so that they are not directed

public space, or

- apply a masking function using software that provides masking

when making recordings, or

- the public area is mechanically covered from the view point of cameras No. 1 and 2,

obsession

- remove cameras 1 and 2.

6. The Authority based on Article 58 (2) point g) of the General Data Protection Regulation

ex officio instructs the Applicant and [the Client] to make this decision final

within 30 days of the divorce, delete the images recorded by cameras No. 1 and 2,

illegal recordings.

7. The Authority based on Article 58 (2) point b) of the General Data Protection Regulation

ex officio condemns the Applicant and [the Client] because they did not provide adequate information

information about their data management related to camera surveillance, thus violating the

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

8. The Authority based on point d) of Article 58 (2) of the General Data Protection Regulation

ex officio instructs the Applicant and [the Client] to make this decision final

within 30 days from the date of divorce, provide Article 13 (1)-(2) of the General Data Protection Regulation information on data management in accordance with paragraph

9. The Authority rejected the Applicant's request for the imposition of a fine, since e the application of a legal consequence does not directly affect the rights or legitimate interests of the Applicant, such a decision of the Authority does not create any right or obligation for him, as a result on this - regarding the application of the legal consequence that falls within the scope of enforcing the public interest in relation to the imposition of fines, the Applicant is not considered a customer under Art. Section 10 (1) on the basis of paragraph 1, and - since the Art. does not comply with paragraph (1) of § 35, e there is no place to submit an application, this part of the submission is an application not applicable.

The Authority nevertheless examined ex officio whether it was justified by the Application and [that Imposing a data protection fine against the customer]. In this context, the Authority is the general Article 83 (2) of the data protection decree and Infotv.75/A. ex officio pursuant to § considered all the circumstances of the case and determined that it was revealed during the present procedure in the event of a violation, a fine is not required.

#### V I . 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.

This decision of the Authority is based on Art. 80-81. § and Infotv. It is based on paragraph (1) of § 61. THE decision of the Akr. Based on § 82, paragraph (1), it becomes final upon its publication. The Akr. § 112, and § 116, paragraph (1) and (4), point d), and on the basis of § 114, paragraph (1) a decision can be appealed through an administrative lawsuit.

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. Section 13 (3) Based on subparagraph a) of paragraph a), the Metropolitan Court is exclusively competent.

The Kp. According to § 27, subsection (1), point b), in a legal dispute in which the court exclusively competent, legal representation is mandatory. The Kp. According to paragraph (6) of § 39 a the effect of delaying the entry into force of the administrative act of submitting a claim there is none.

The Kp. Paragraph (1) of Section 29 and, in view of this, CXXX of 2016 on the Code of Civil Procedure. is applicable according to § 604 of the Act, Eüsztv. According to Section 9 (1) point b), the customer legal representative is 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 on the possibility of a request to hold a hearing in Kp. Section 77 (1)-(2) based on paragraph

The amount of the fee for the administrative lawsuit is determined by Act XCIII of 1990 on fees. law (hereinafter: Itv.) 45/A. Section (1) defines. Payment of the fee in advance from under the Itv. Section 59 (1) and Section 62 (1) point h) exempt the procedure initiating party.

The Akr. According to § 132, if the Respondent and [the Client] in the final decision of the Authority did not comply with the stated obligation, it is enforceable. The Authority's decision in Art. Section 82 (1) according to paragraph, it becomes final with the communication. The Akr. According to § 133, the execution - if the law or government decree does not provide otherwise - the decision-making authority

16

orders. The Akr. Pursuant to § 134, enforcement - if you are a law or government decree in municipal authority cases, the local government decree does not provide otherwise - is carried out by the state tax authority.

Budapest, February 1, 2022.

Dr. Attila Péterfalvi

c. professor

president