NAIH-1006-3/2022

NAIH-4360/2021

Case number:

Antecedent:

Subject: decision

ex officio

data protection

in procedure

starter

official

H A T A R O Z A T

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

hereinafter: Customer) started on May 11, 2021 in relation to camera data management

Due to the circumstances revealed during the official inspection, the official data protection investigation was initiated on July

2, 2021

in procedure

1. states that

the. the Client has violated the handling of the personal data of natural persons

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

95/46/EC

Regulation (EU) 2016/679 on the repeal of the Directive (a

hereinafter: General Data Protection Regulation) points b) and c) of Article 5 ("purpose limitation" and

"data saving") when in the "office-customer waiting room" and "kitchen" rooms of its headquarters

set the angle of view of the installed camera so that they are suitable for the employees

unjustified surveillance and are not only aimed at assets to be protected.

b. The Customer has violated Article 6 (1) f) of the General Data Protection Regulation

point, since instead of referring to the legitimate interests of the data controller, the employees

his contribution formed the legal basis for the operation of the chamber system.

c. The Customer has violated Article 13 (1)-(2) of the General Data Protection Regulation,

when he did not properly inform his employees about the camera data management taking place there

about his circumstances.

2. obligates the Customer to

the. the viewing angles of the cameras installed in the "office-customer waiting room" and "kitchen" rooms at the headquarters

change it so that they are not suitable for employees unreasonable

to observe and in accordance with

personnel and

with the purpose of asset protection.

be the system

b. Change the data management policy of the camera system so that it does not a

the consent of employees, but the legitimate interest of the data controller should form the system

the legal basis of its operation and therefore carry out the necessary interest assessment

test.

c. Change the privacy policy of the camera system to comply with it

in paragraphs (1)-(2) of Article 13 of the General Data Protection Regulation and III./3 of the decision

as contained in point

……

……

1055 Budapest

Falk Miksa utca 9-11

Phone: +36 1 391-1400

Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu

3. due to the above infringements, the Customer shall, within 30 days from the date of this decision becoming final,

within days

HUF 500,000, i.e. five hundred thousand forints

obligates you to pay a data protection fine;

4. orders the personal data and Customer identification data to be the final decision

its disclosure by covering up (anonymizing) it.

The fine is a centralized revenue collection purpose settlement by the Authority

HUF account

(10032000-01040425-00000000 Centralized direct debit account IBAN: HU83 1003 2000 0104

0425 0000 0000) must be paid by bank transfer. When transferring the amount, NAIH-1006/2022.

FINE. number must be referred to.

If the obligee does not fulfill his obligation to pay the fine within the deadline,

must pay a late fee. The amount of the late fee is the legal interest, which is a

it is the same as the central bank base rate valid on the first day of the calendar semester affected by the delay. THE

late fee to the forint settlement account of the Authority's centralized revenue collection purpose

(10032000-01040425-00000000 Centralized collection account) must be paid.

In the event of non-payment of the fine and late fee, the Authority orders the decision, the fine

and the execution of the late fee.

There is no place for administrative appeals against this decision, but it is subject to notification

Within 30 days with a letter of claim addressed to the Capital Court in a public administrative case

can be attacked. The letter of claim must be submitted electronically to the Authority in charge of the case

forwards it to the court together with its documents. The request to hold the hearing must be indicated in the statement of claim

must For those who do not receive a full personal tax exemption, the administrative court fee is 30

HUF 000, the lawsuit is subject to the right to record the levy. In the proceedings before the Metropolitan Court, the legal

representation is mandatory.

I.

History, clarification of the facts

1. Content of the notification received by the Authority

I N D O C O L A S

[…] (hereinafter: Kft.) submitted a complaint to the Authority by post on April 22, 2021. THE

submitted that the Kft. and […] private individual in 1/2 – 1/2 ownership share

owners of the property under […]. The property is used as a car repair shop. THE

litigation in connection with property disputes between owners and the termination of joint ownership

procedure is in progress.

The Client under the management of [...] in the property also carries out car repair activities. The

real estate functions as the Customer's location and thus appears in the company register.

2

The representatives of the Kft. wanted to start renovation works on March 7, 2021 in the above

on the property, or to start moving into it. This is only by violating the doors, respectively

they managed to do it with the help of the police. Upon entering the property, they were confronted by Kft.

representatives with the fact that a recently installed camera system is operating there.

[...] the co-owner of the property and also the Customer's manager in relation to the cameras, no

was able to answer who owned them and in what quality

equipped. According to him, he transmits the live images to the phone of his business partner […]. Since Kft., as

the co-owner of the property was not informed in advance or asked about the cameras

about its equipment, and no informational materials/boards were installed on it

property, so he asked the Customer's manager to dismantle them or arrange the

system-related questions, access. On March 16, 2021, representatives of the Kft. Client

in the presence of the executive, the cameras were disconnected from the power supply and communication

from line.

Later on April 10, 2021, representatives of the Kft. noticed in the property that the cameras were again

they work and there are still no warning signs for the cameras, no data management

information sheet. The representatives of the Kft. again asked the Customer's managing director to take action with the camera system

regarding its legal operation, or dismantle them. A worthy answer, according to him

they didn't get it.

The complainant Kft. made the above statements with the title deed of the property, addressed to the Customer's executive

he supported it with an e-mail notice and photos taken from the cameras. The complainant

he also attached the decision of the Clerk of […] No. […] for property protection submitted by the Client

on the rejection of his request for a procedure.

The complainant is investigating the above - in his opinion illegal - camera data management

requested the Authority to conduct it.

2. They were determined during the official inspection ordered on the basis of the petition

1) The Authority in connection with the surveillance of the Customer's workplace by camera on May 11, 2021

NAIH-4360-3/2021. started an official control on the case file number from the point of view of its assessment,

whether the Customer has fully complied with the provisions of the general data protection regulation

obligations. On the initiation of the official inspection, the Authority simultaneously a

NAIH-4360-2/2021 also informed the Kft that filed the complaint. case file number.

2) In order to clarify the facts, the Authority NAIH-4360-3/2021. No. dated May 11, 2021

ordered the Client to make a statement and provide documents, which he did within the deadline

answered.

Based on the Customer's statements to the order, it can be established that he is indeed a surveillance officer

installed cameras in the area of the above property where work is carried out (vehicle repair, maintenance)

is also ongoing. Based on the statement, the surveillance cameras were installed on March 5, 2021. THE

the decision to install the system was made by [...] (Customer's managing director and 75% co-owner)

because he owns 1/2 of the observed property. The installation

as the reason, the Customer indicated that all the workshops located in the property used to have entrance doors

the locks on the door were damaged, probably with the intention of breaking in. To the workshop after that
it was impossible to get in due to the complete destruction of the locks, police action was also taken in the matter.
3
As an additional installation reason, the Customer indicated the protection of objects and tools in the workshop.
The workshop doors open directly onto the public area, there is no fence or yard, the area is fenced off
due to its nature, it cannot be implemented.
The customer also stated that on March 7, 2021 […] and […] (complainant Kft., as real estate
co-owner representatives) dismantled the workshop entrance and interior doors for renovation. the doors,
since the property was no longer lockable, they were screwed in with OSB sheets. After these events
an internal data recording unit was added to the cameras. In response to the Authority's question in this regard, the Client
designated a natural person named […] as data controller, who is a 25% co-owner of the Customer.
Based on the customer's statement, the camera system only monitors the internal area of the property, public area
no. Only people working there, customers and other strangers are allowed to stay in the workshop
persons may not stay in the property since March 6, 2021. A worker in the workshop
number of people: 4 full-time employees, and 2 casual employees.
According to the customer, the employees were informed in writing about the camera system
on its introduction, which they accepted with their signatures. Signed by all employees of the customer
He sent a copy of the "contributing statement" to the Authority. The employee is personal
information (name, date of birth, residential address, SZIG number) can be found on a uniform declaration
according to text:
"[employee personal data] I certify with my signature that the […] number
in the property below as a closed chain operating for the purpose of asset protection as an employer
to be monitored with a camera system, during which it will also occur during my working hours
convey an image. I have received the information about the system and am aware of its contents
I buy it, I don't want to live with an excuse. [date, then signature of employee and Customer
corporate signature.”

In addition to the above, a camera pictogram on the door of the workshop warns of the operation of the system in 2021.

from May 8.

Recordings are stored in the recording unit in the camera and on a cloud basis, the internal

rooms (kitchen, warehouse-office, customer waiting-office) cameras for 3 days, while the one in the workshop

cameras record 7 days. According to the Customer, it is not possible to monitor a live image, otherwise it is recorded

recordings […] (25% owner of Customer) can access and view them, […] (Customer

with the permission of its 75% owner).

The customer sent the images transmitted by the cameras to the Authority, as well as the property by hand

drew a map of the site, marking the viewing angles of each camera.

3) Later the Authority NAIH-4360-5/2021. No. dated June 7, 2021 again

invited the Client to make a statement and provide documents, which he also did within the deadline

answered.

The customer stated that he has access to the camera surveillance system

with the data protection policy and data protection information, which were also sent in copies by

To authority. The regulations are effective from May 8, 2021.

4

information sheet" document

"camera surveillance system data management

a) A

main

his findings are as follows: The primary purpose of using the system is human life, physical

integrity, protection of personal freedom, safekeeping of dangerous substances, business, payment, banking and

protection of securities secrecy and asset protection. The purpose of using the system is not a

influencing the behavior of employees. A Customer has been designated as a data controller,

however, the name and contact details of [...] were indicated as contact information.

They were marked separately for the total of six cameras

data management purposes (which is uniformly property protection) and the monitored area. The recordings

According to the information, the storage period is uniformly three working days, which is in extremely justified cases

It can be extended up to 30 days. After the storage time, the recordings are automatically deleted

are (overwritten). The method of data storage is electronic.

The person entitled to review the recordings [...], which is in case of "theft, material damage".

possibility, only "in case of event". The legal basis for data management is only as follows:

information that "the legality of the data management of the system does not require the observed

consent of persons".

Among the laws that form the basis of data management are the General Data Protection Regulation and the

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

hereinafter: Infotv.) about public documents, public archives and private archival material

LXVI of 1995 on protection Act, the general document management of bodies performing public duties

335/2005 on its requirements. (XII. 29.) Government decree, electronic commerce

services as well as the

some services related to society

CVIII of 2001 on questions Act and Act C of 2003 on Electronic Communications

was also marked.

b) The document called "camera surveillance system data protection and data management policy".

it largely repeats the provisions of the information described in the previous point a). Difference between the two,

that the regulation has a separate chapter on the legality of the application of the system, which word

received according to

from legislation: XLI of 2012. law a

on passenger transport services, LXIII of 1999. Act on the Supervision of Public Areas, 2005

CXXXIII. law on personal and property protection, as well as private detective activity

about its rules. These additional laws are listed in addition to those mentioned in point a).

also in the "legislation on which data management is based" section of the regulation.

The regulations also include Infotv. general provisions adopted from its invalid text

also about the obligation to register in the data protection register.

The regulations contain different provisions regarding the storage time of the recordings

compared to information. According to them, the Customer can "generally" use the camera recordings for 3 working days

stored, but in the case of workshop cameras, the storage time is 7 days. The storage time is extraordinary

due to circumstances, its extension to 30 days was indicated here as well.

Regarding the legal basis of data management, the regulations also only refer to the fact that no

the consent of those concerned is required.

In addition to the above, the regulation is short and general, so it does not apply to the operation of the specific system

contains regulations on data security and the handling of data protection incidents.

contains the following

informative

quotes

5

In addition, it also generally contains regulations on the legal status of the data protection officer and

in relation to his duties, but does not designate his person.

c) The customer also forwarded to the Authority a "data management agreement" dated May 20, 2019

information" document. This document provides general data protection information

contains in relation to the personal data managed by the Customer, on that website, direct

personal data handled in the course of marketing activities and in connection with general business operations

provides information about data to those concerned. The information therefore does not apply to the camera system.

4) In addition to the above, the Customer has stated that the Customer [...] for the cameras' recordings by telephone

accessed through an application. In the case of an event, the recording takes place with the consent of […]

view pictures. Such a case has not yet taken place until the declaration.

Regarding the recording of the "office-customer waiting" room, the Customer submitted that he is currently there

administrative work is in progress. The cash register and (bank) card reader are located in this room,

and also the till.

3. Facts established during the official data protection procedure

In addition to the further clarification of the facts, the general data protection regulation in the case

Due to the further necessary investigation of the customer's presumed violation of obligations, the

the Infotv. With regard to Section 60 (1), on the initiation of official data protection proceedings by the Authority

decided on July 2, 2021, about which NAIH-4360-8/2021. notified the Customer at the number a

according to the returned receipt, it was received on July 7, 2021.

1) In order to further clarify the facts, the Authority NAIH-4360-9/2021. No. July 12, 2021-

invites the Customer to make another statement and serve documents, for which it is, by order dated

replied within the deadline.

According to the customer's answer, there is no consideration of interests in relation to the camera system

with a test. Furthermore, the client emphasized once again that the system is not aimed at employees

monitoring, only asset protection.

Customer in relation to the fact that the hazardous substances included in the data management information sheet

safeguarding, the protection of business, payment, bank and securities secrets, how is the

through the use of a camera system, stated that the monitored property is stored in the

with business

card reader,

computers, as well as the key to the storage of external hazardous materials. The customer also stated

that there is no work in the kitchen area, only rest and dining activities,

in addition, the company's armor cartridge is located here.

Phone application for viewing recordings (YCC365, version number: 4.1042.5.050)

it is also suitable for viewing live images, but no one checks this with the Customer, it is only charged in the event of an event

in retrospect, the recording recorded on cloud-based storage.

The Authority also had a question as to why statements of consent were prepared by the employees

on the part of the system itself, when the data subject's consent cannot form the legal basis for data management

nor according to the data protection policy. The Customer replied that before installing the cameras

consulted with the employees, who agreed to equip them for property protection purposes.

related documents, the cash register,

cash register,

6

These consents were recorded in writing to avoid possible later disagreements

because of

2) The Authority's internal IT security expert NAIH-4360-11/2021. experts on case file number

created an opinion the smartphone application used by the Customer (YCC365) is essential

properties that the Customer uses to view camera images.

According to expert opinion, the app can be installed on smartphones by iOS and Android users

is available for both, and can be used to transmit and store real-time video. The

when using the application for the first time, you must register an account using your e-mail address, "Sign Up"

(Registration) by clicking on it. After that, connected to a Wi-Fi network and using an application

by scanning the generated QR code with the chosen camera, after successful connection in the application

the live image is displayed.

The pre-image transmitted by the camera, as well as additional functions (e.g. camera control, tilt, zoom)

are also available remotely. The application includes 30 days of cloud-based hosting for free

can be tried, after this time you can prepay for it. The cloud service is provided by Amazon AWS

supports, all video and audio are stored in amazon web services; US-EU Safe

Harbor protocol with encryption. After inserting an SD card into the camera, the camera records the videos

Saves to SD card while continuously deleting old ones.

The Authority NAIH-4360-12/2021. on the general administrative order with its order with case file no

solo 2016 CL. on the basis of § 76 of the Act (hereinafter referred to as Ákr.) sent the Customer a

expert opinion in order to exercise your rights provided in this section. Customer a

according to the returned receipt, he received the order on September 24, 2021, from then until today

no comments were received by the Authority.

3) The Authority finally NAIH-1006-1/2022. on the case file number, the Customer declared that a

In the business year 2021, what was the total amount of the net sales revenue, considering

to the fact that the investigated data management affected this year, as well as the general data protection regulation

83 for the purpose of considering aspects of the administrative fine that can be imposed. Customer

based on his statement, in 2021 the net sales revenue of his sales was HUF […].

II.

The Akr. On the basis of § 99, the authority - within the framework of its powers - checks the legislation

compliance with the provisions contained, as well as the fulfillment of the provisions of the enforceable decision.

The Akr. Based on point a) of paragraph (1) of § 101, if the authority finds a violation during the official inspection

experiences, initiates the official procedure. Infotv. Section 38 (3) and Section 60 (1).

based on Infotv. personal data within the scope of duties according to § 38, subsections (2) and (2a).

in order to enforce the right to data protection, it conducts official data protection proceedings ex officio.

The Akr. According to § 104, paragraph (1), point a), the Authority ex officio in its area of competence

initiates the procedure if it becomes aware of the circumstances giving rise to the initiation of the procedure;

based on paragraph (3) of the same paragraph, the ex officio procedure is the first procedural act

begins on the day it is completed, notification of its initiation to the known customer can be omitted if it is

the authority makes a decision within eight days after the initiation of the procedure.

Applicable legal provisions

7

Pursuant to Article 2 (1) of the General Data Protection Regulation, the subject of the procedure

the general data protection regulation shall be applied to data management.

According to Article 4, point 1 of the General Data Protection Regulation, "personal data": you are identified

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

a natural person who, directly or indirectly, in particular an identifier, for example

name, number, location data, online identifier or physical, physiological,

one or more related to your genetic, intellectual, economic, cultural or social identity

can be identified based on a factor.

Based on Article 4, point 2 of the General Data Protection Regulation, "data management": on personal data

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

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

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

by way of making it available, coordination or connection, restriction, deletion,

or destruction.

Based on Article 5 (1) point b) of the General Data Protection Regulation, personal data

should only be collected for specific, clear and legitimate purposes and should not be processed

in a manner inconsistent with these purposes; in accordance with Article 89 (1) no

is considered incompatible with the original purpose for the purpose of archiving in the public interest, scientific

and further data processing for historical research or statistical purposes ("for purpose

constraint").

Based on Article 5 (1) point c) of the General Data Protection Regulation, personal data is

they must be appropriate and relevant for the purposes of data management

be and a

they must be limited to what is necessary ("data saving").

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

for compliance with the basic principles contained in paragraph, and must also be able to comply

for verification ("accountability").

According to Article 6 (1) point f) of the General Data Protection Regulation, personal data

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

data management is for the enforcement of 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 of the General Data Protection Regulation

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

at the time of obtaining personal data, the following is made available to the data subject

all 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 a third party

legitimate interests of a party;

e) where appropriate, 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

and compliance of the Commission

wishes for

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

reference to 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 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 a basis or a prerequisite for concluding a contract, and whether the person concerned is obliged to the personal

provide data,

it can work

failure to provide data;

with their possible consequences

and 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.

2005 on the rules for personal and property protection and private detective activity.

year XCCCIII. Act (hereinafter: Szvtv.) is not applicable according to § 30, paragraph (3).

electronic surveillance system in a place where surveillance may violate human dignity,

so especially in changing rooms, fitting rooms, washrooms, toilets, hospital rooms and social services

in the residence of the institution.

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

according to the employee's personal right can be limited if the limitation is the employment relationship

absolutely necessary for a reason directly related to its purpose and proportional to the achievement of the goal. THE

personal

furthermore

the employee in advance in writing about the circumstances supporting its necessity and proportionality

must be informed.

Mt. 11/A. According to § (1), the employee's conduct related to the employment relationship

can be checked among Within this framework, the employer can also use a technical device, as per

informs the employee in advance in writing.

Infotv. Based on point a) of section 61 (1), the Authority in sections (2) and (4) of section 2

in connection with specific data management operations in the general data protection regulation

may apply specific legal consequences.

on the method of limiting the right,

conditions and expected

duration,

his activity violated the provisions of the decree,

Based on points b) and i) of Article 58 (2) of the General Data Protection Regulation, the supervisory

authority, acting in its corrective powers, condemns the data manager or data processor if

data management

and Article 83

appropriately imposes an administrative fine, depending on the circumstances of the given case, e

in addition to or instead of the measures mentioned in paragraph Paragraph (2) of the same article

on the basis of point d), the supervisory authority instructs the data controller acting in its corrective powers

or the data processor to perform its data management operations - in a specified manner and

within a specified time - bring it into line with the provisions of the decree.

The conditions for imposing an administrative fine are set out in Article 83 of the General Data Protection Regulation.

article contains. Infotv. 75/A. According to § 83 of the General Data Protection Regulation, the Authority

in paragraphs (2)-(6) of Article

taking into account

practice, especially with the fact that in the legislation on the management of personal data

or regulations defined in a mandatory legal act of the European Union - for the first time

in case of violation, to remedy the violation - with Article 58 of the General Data Protection Regulation

in accordance with - takes action primarily with the warning of the data manager or data processor.

included powers of the principle of proportionality

III. Decision

1. The legal basis of the examined data management

1) Based on the definition contained in Article 4, Point 1 of the General Data Protection Regulation, a

a person's face and likeness are considered personal data, the taking of the picture, as well as the data

and any operation performed is classified as data management based on point 2 of Article 4.

Given that the viewing angles of the cameras were designed to be the observed

in the area of the premises and in addition to the assets located there, the person staying in the building under […]

employees are also monitored based on the documents sent to the Authority, the workplace

the rules regarding camera surveillance must also be taken into account for the legality of the case

regarding his judgment. When assessing this, the following labor law rules are applicable.

Pursuant to point a) of § 42, paragraph (2) of the Labor Code, the employee is obliged to, based on the employment contract

to perform work under the direction of the employer. In accordance with this, Section 52 (1) b) of Mt.

and c) defined as a basic duty of the employee that the employee

is obliged to be available to the employer during his working hours and his work is generally expected

with expertise and care, the rules, regulations, instructions and

to perform according to custom. In order to comply with these legal obligations, Mt. 11/A. § (1)

paragraph provides an opportunity for the employer to provide the employee with the employment relationship

check in the range of related behavior. This right necessarily goes hand in hand

by handling personal data.

Data management related to employer control from the provisions of Mt., the employment relationship
data management arising from its nature, independent of the employee's consent. With consent
in this context, it should be noted that its general data protection regulation
according to its definition1, it must be voluntary. Regarding the voluntary contribution

1 Article 4, point 11 of the General Data Protection Regulation: ""consent of the data subject": voluntary, specific and
based on adequate information and a clear statement with which the relevant statement or confirmation
indicates through an unmistakably expressive act that he gives his consent to the processing of his personal data."

at the same time, it was created according to Article 29 of the already repealed data protection directive2
In several resolutions of the Data Protection Working Group3 (hereinafter: Data Protection Working Group).
also explained that the volunteer can be questioned in the employee-employer relationship
possibility of contribution. In the world of work, instead of the data subject's consent, there is therefore another legal basis, a
the use of data management based on the employer's legitimate interests is justified.
Pursuant to the legal basis of legitimate interest in Article 6(1)(f)4 of the General Data Protection Regulation
therefore, personal data can be processed if the data is managed by the data controller (or
third party) is necessary to assert its legitimate interest, unless these interests
it is preceded by the data subject's right to the protection of personal data.
It is essential that the employer, as a data controller, has a consideration of interests when referring to this legal basis
must carry out.5 Carrying out the interest assessment is a multi-step process during which
the legitimate interest of the data controller, i.e. the employer, as well as the counterpoint of the weighting must be identified
data subject, employee interest, affected fundamental right, and finally based on the weighting
it must be established whether personal data can be processed. If the consideration of interests
as a result, it can be established that the legitimate interests of the employer precede those of the employees
the right to the protection of personal data, the camera system can be operated as such.
From the "principle of accountability" according to Article 5 (2) of the General Data Protection Regulation
however, the employer must prove that it is electronic

monitoring system is compatible with the principle of purpose-bound data management and the consideration of interests its outcome resulted in the primacy of the legitimate interest of the data controller. This is the requirement defines the framework for the purpose of an electronic monitoring system in the workplace operate.

The Authority also notes here that during the carried out consideration of interests, the Client also you must consider that the undivided community property you wish to observe is complete why the observation of its territory is absolutely necessary for the specified purpose.

2) In the data protection regulations sent to the Authority ("camera surveillance system data protection and data management regulations"), the camera operator was not specifically identified the legal basis for monitoring, it is just that in the case of such data management, the data subject cannot form it consent is the legal basis. Compared to this, the Customer is on behalf of each employee involved obtained declarations of consent, which were authenticated by the signatures of the persons concerned.

2 on the protection of individuals with regard to the processing of personal data and the free flow of such data European Parliament and Council Directive 95/46/EC

3 The Data Protection Working Group is, before the start date of the application of the general data protection regulation independent European consultant dealing with issues related to data protection and privacy protection was a body, replaced by the European Data Protection Board.

4 Article 6 (1) point f) of the General Data Protection Regulation: "The processing of personal data only when and to the extent is legal if at least one of the following is met: the data processing is authorized by the data controller or a third party it is necessary to assert its interests, unless the interests of the person concerned take precedence over these interests interests or fundamental rights and freedoms that require the protection of personal data, especially if affected child."

5 The Data Protection Working Group 6/2014 provides assistance in carrying out the interest assessment. number, the data controller opinion on the concept of legitimate interests according to Article 7 of Directive 95/46/EC, in which the general they can also serve as an interpretation during the period of application of the data protection decree. The opinion is available

from the following link:

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

11

in writing

During the clarification of the facts, the Authority asked why statements of consent were made

on the part of employees, when the data subject's consent cannot form the legal basis for data management

nor according to the system's own data protection policy.6 The Customer replied that the cameras

prior to installation, he consulted with the employees, who agreed for the purpose of asset protection

for installation. These contributions

possible later ones are also recorded

to avoid disagreements. The customer also declared that he does not have the

in relation to the camera system with an interest assessment test.

Based on the above, despite the provisions of the data protection regulations, the Customer is in practice

based on the consent of those concerned, the operation of the camera surveillance system is based on its own right

instead of his interest. This is supported by the consent statements requested, as well as the interest assessment

lack of test.

However, based on the provisions of the previous subsection III./1./1) of the decision, a workplace cameraman

the use of a monitoring system cannot be based on the employees' consent. It's like that

systems may be operated at the workplace based on the legitimate interests of the data controller.

In addition, the regulations have taken verbatim quotes about the legality of the system's application

contains legislation7 that is completely in terms of camera data management

are irrelevant. These additional laws are listed under the "data management basis

legislation" in the regulation. The regulations also include Infotv.

general provisions adopted from the invalid text8 are included in the data protection register

also about the registration obligation.

Based on the above, it is clear from the regulations created in connection with the operation of the system that the Customer

randomly stitched together by a template used as a probably invalid

data management regulations and based on randomly selected legal references.

Here, the Authority states that in the data management regulations, the data controller has exactly

you must be able to indicate the legal basis for data management based on the applicable legal provisions,

by haphazardly listing various legal references, he is not aware of this obligation

to escape

The customer therefore violated Article 6 of the General Data Protection Regulation by operating the camera system.

point f) of paragraph (1) of Article, as it is the consent of the employees instead of the legitimate interest

formed the legal basis for the operation of the system.

6 NAIH-4360-9/2021. 6) of order no

7 - LXVI of 1995 Act on public documents, public archives and the protection of private archive material,

- 335/2005. (XII. 29.) Government Decree on the general requirements for document management of bodies performing public

duties,

- CVIII of 2001 law with electronic commercial services and the information society

about some issues of related services,

- Act C of 2003 on electronic communications,

- XLI of 2012 law on passenger transport services,

- LXIII of 1999 law on the supervision of public areas,

- CXXXIII of 2005 Act on personal and property protection, as well as the rules of private detective activity.

8 The obligation to register in the data protection register previously maintained by the Authority is Infotv. July 2018

27 was deleted from its effective text. Currently, the Authority does not keep such records, so that is it

data controllers do not have to and do not have the option to log in.

2. The purpose of the examined data management

1) Data management in the customer's answers to the Authority and in the attached documentation

aims to protect the safety of the buildings and the assets located there, and a

protection of hazardous materials and security of payment operations, as well as personal protection purposes marked. The purpose of operating the camera system is therefore not the work of the employees monitoring and influencing, but personal and property protection.

In this regard, it is important to mention that camera surveillance in the workplace is absolute its limit is the respect for human dignity, so cameras are used by the employees and the not to operate for the permanent observation of their activities without an express purpose may. It is also considered illegal to use an electronic monitoring system that whose purpose is to influence the behavior of employees at work, the employees permanent monitoring and control with cameras. This is because it is for verification purposes monitoring typically violates the necessity-proportionality principle, since the employer has many there is another way to live in Mt. 11/A. with the right of inspection according to paragraph (1) of § So that's why it is not possible to operate cameras that only show employees and their work activity is monitored on a permanent basis. Exceptions are workplaces where a the life and physical integrity of employees may be in direct danger, so it can be operated exceptionally camera in, for example, an assembly hall, a smelter, in industrial plants or other sources of danger in facilities containing However, it should be emphasized that only in that case operable camera in order to protect the life and physical integrity of employees, if there is danger actually exists and is immediate, that is, the possible danger cannot be constitutional acceptable data management purpose. However, the employer must prove all of this in a balance of interests test.

In the case of monitoring for the purpose of property protection, the employer must also do so to prove it during the consideration of interests, that there are actually circumstances that justify it the placement of some cameras and other means cannot ensure the goal to be achieved. Asset protection in the case of surveillance for the purpose of monitoring, another important requirement is that the employer pay particular

attention to

it must be such that the angle of view of the given camera is basically aimed at the asset to be protected,

and, as a result of the above, do not monitor the work of employees

suitable tool.

In addition, it is also not possible to use an electronic monitoring system in a room that

which was designated for the employees to spend their breaks between work. An exception to this

may be the case if there is some valuable asset to be protected in this room,

in connection with which some employer's interest can be justified (for example, employees

the equipment was damaged several times and the employer had to pay for the damage). In this

in this case, a camera can be placed in the room for this specific purpose, but then the

the employer - following the principle of data saving - also needs special attention

that the angle of view of the camera can only be directed at the asset to be protected.

2) Based on the customer's answers and the images sent by the placed cameras

it can be established that they are:

- The workshop for car assembly work in the building was stored there

cars and tools are monitored (3 cameras).

- Observes a warehouse and the goods, tools and parts stored there (1

piece of camera).

- He observes the waiting room and office for receiving customers, where the camera

the cash register and bank card reader terminal (1 camera) also fall into its field of vision.

- Monitors the kitchen area, directed at the dining table (1 camera).

seal

in connection with its activities

According to the judgment of the Authority and according to the legal provisions referred to above, the Customer

for personal and property protection purposes indicated by the 3 cameras in the workshop

transmitted image, and the image transmitted by 1 camera monitoring the warehouse

can be answered. Work in these rooms is dangerous

(car mechanic

activity), as well as high-value assets stored there (cars, tools, etc.)

can justify its camera surveillance, in the event that the proportionality of this is determined by the Customer a

can prove it during an interest assessment.

The customer also has asset protection purposes in connection with the camera surveillance of the customer waiting room and

cash register

marked, as well as the safekeeping of dangerous substances, business, payment, banking and securities secrets

protection as well. The reason for this is that the cash register, till, card reader, computers are stored here,

as well as the key to the storage of the external dangerous substance. Based on the Authority's position, in the customer

waiting room

the angle of view of the installed camera is suitable for seeing the employees and the there

arriving customers, customers The customer is entitled to view the camera image on his employee

check through The reason for this is that not only the cash register is in the camera's field of view,

a workstation with a card reader and the key cabinet, but almost the entire room -

including the customer service desk, he observes. Constant monitoring of this last part of the room

neither the protection of assets nor the safeguarding of dangerous substances and the protection of business and payment

secrets

purpose is not justified. The Authority notes that bank and securities marked by the Client are confidential

protection Customer

it cannot even arise, as it is not a credit institution

business undertaking activities.

Finally, in connection with the observation of the kitchen, the Customer referred to the fact that there was no work there

going on, only rest and dining activities, in addition, the company's armor cartridge is also located here.

In connection with the observation of this room, the Authority determines that the angle of view of the camera is that

it is aimed at the dining table, and the mentioned armor cartridge does not fall into it. By the camera

therefore, the transmitted image is not suitable for carrying out surveillance for the purpose of personal and property

protection,

on the other hand, employees spend their breaks (meals) here. Camera angle

therefore, it is suitable for unwarranted surveillance of employees during their breaks,

on the other hand, it cannot fulfill the specified asset protection purpose, as it does not fall into that armor cartridge

into it.

3) Based on the above, the Authority determines that the "office-customer waiting room" of the Customer's headquarters and

The viewing angle of the camera installed in the "kitchen" premises is suitable for the employees and is unreasonable

monitoring, so it is not compatible with the original goal of personal and property protection. THE

data management via camera therefore violates Article 5 (1) of the General Data Protection Regulation

the principle of "boundedness to purpose" according to paragraph b).

In addition, since the visual text of the mentioned cameras is not aimed at the assets to be protected, but

the image it conveys includes a wider spectrum of vision, thus enabling the

complete monitoring of premises as well, according to the Authority's point of view, the principle of data saving - that

Article 5 (1) point c) of the General Data Protection Regulation - is also violated by the Respondent

data management.

14

In view of the above, the Authority called on the Applicant in the operative part of this decision,

that the viewing angles of the cameras installed in the "office-customer waiting room" and "kitchen" rooms of your premises

set them up so that they are not suitable for unwarranted surveillance of employees and

serve only property protection purposes.

3. Informing the affected parties about the investigated data management

1) In the case of data management related to workplace camera surveillance

essential

requirement that employees about data management are appropriate, transparent and easy

receive interpretable information. In this regard, the following must be taken into account:

Pursuant to Section 9 (2) of the Mt.: "On the manner, conditions and

about its expected duration, and about the circumstances supporting its necessity and proportionality a

the employee must be informed in writing in advance." Mt. 11/A. According to § (1), if a

the employer also uses a technical device to check the employees, in writing in advance

must inform them.

Article 13 (1)-(2) of the General Data Protection Regulation states that data management

what about

information must be made available to employees

in relation to data management.

In the case of data management related to camera surveillance, the General Data Protection Regulation

according to the system of requirements prescribed by

must be informed of circumstances:

- about the person operating the electronic monitoring system (legal or natural

with the exact name of the person) and contact details,

- the contact information of the data protection officer, if the data controller has appointed one

person,

- about the location of the individual cameras and the purpose they serve in relation to them

about the observed area, object, or whether you are direct with the given camera

does the employer carry out fixed monitoring,

- on the legal basis of data management,

- on the definition of the legitimate interest of the data controller,

- on the duration of storage of the recording,

- about the range of persons entitled to access the data, and whether the recordings

to which persons and bodies, and in what cases can the employer forward it,

- about the rules for reviewing the recordings, and that the recordings

for what purpose can the employer use it,

- about

what the employees are like

rights

they deserve it

the

electronic

in connection with a surveillance system and how they can exercise their rights,

- that it is

in the event of a violation of their rights

they can use legal enforcement tools, including turning to the Authority

about the possibility.

information self-determination

15

you know

justify to employees why

Regarding the obligation to provide information, it is also necessary to point out that the employer

for each camera, you must indicate exactly what kind of camera it is

for which purpose it was placed in the given area and to which area and equipment the camera's angle of view is directed.

The employer with this

can be considered

monitoring of the given area is necessary. The practice is not acceptable when a

the employer only informs the employees in general that it is electronic

uses a monitoring system in the workplace.

The following are based on the documents provided and sent by the client at the request of the Authority

can be determined from the information related to the operation of the camera system.

The main findings of the document called "data management information for the camera surveillance system".

are as follows: The primary purpose of using the system is human life, physical integrity, personal

protection of freedom, safeguarding of dangerous substances, business, payment, banking and securities secrecy

protection and asset protection. The system is not aimed at employees

influencing his behavior.

A Customer has been designated as a data controller. The name and contact details of […] have been added as contact

details

for indication.

They were also marked separately for the six cameras in total

data management purposes (which is uniformly property protection) and the monitored area. The recordings

According to the information, the storage period is uniformly three working days, which is in extremely justified cases

It can be extended up to 30 days. After the storage time, the recordings are automatically deleted

are (overwritten). The method of data storage is electronic.

The person entitled to review the recordings [...], which is in case of "theft, material damage".

possibility, only "in case of event". The legal basis for data management is only as follows:

information that "the legality of the data management of the system does not require the observed

consent of persons".

Additional legislation specified by the customer in the information sheet (Act LXVI of 1995, 335/2005

(XII. 29.) Government Decree, CVIII of 2001 Act and Act C of 2003) on data management

are completely irrelevant, as they are not in relation to camera data management

contain applicable regulations. In any case, the purpose of referring to them was not achieved

to be indicated in the information sheet, so listing them is completely unnecessary.

The customer also forwarded to the Authority a "data management agreement" dated May 20, 2019

information" document, which, however, does not apply to the camera system, thus

the Authority does not make any further findings in this regard.

2) In relation to the above, it can be established that the information on data management contains errors

the legal basis of data management, as it is not clearly indicated, only the consent of the data subject

refers to the need for its acquisition. Here, for the Customer, it is the legal basis for data management

point f) of Article 6 (1) of the General Data Protection Regulation, i.e. the legitimate interest of the data controller

should have indicated, as stated in Decision III/1. was also explained in The legitimate interest

and in the case of data management based on

results, however, according to the Customer's statement, he does not have any. In addition, the

information, similar to the system's data management regulations, completely irrelevant legislation

and also indicates goals (see point III./1. of the legal basis and point III./2. of the decision

in terms of goals).

In addition to the above, the data management information sheet does not contain information about the employees

what rights they have in connection with the electronic monitoring system and in what way

can exercise their rights, and also that in connection with the enforcement of their rights to the Authority

they can turn.

Article 13 (1) of the General Data Protection Regulation stipulates that the data controller a

at the time of obtaining personal data, you must provide the data subject with the

all of the listed information.

In relation to the above, the Authority concludes that the information does not meet the general requirements

of data protection Article 13, paragraphs (1)-(2) due to the following aspects:

- the actual legal basis for data management (the legitimate interest of the data controller) has not been indicated,

- the prospectus does not include the interest assessment test,

- the information sheet refers to legislation irrelevant from the point of view of data management,

- the information also indicates purposes unrelated to data management (business, payment, banking

and protection of securities secrets),

- the information sheet does not contain information about the rights of the data subjects and the possibilities of legal

enforcement

information.

The Customer forwarded to the Authority a photograph that appears to be pictographed

placed a warning sign at the entrance to the business premises for camera surveillance

to be called on May 8, 2021. Because additional information is provided

requirement that the employer is obliged to post a warning sign about the fact that

applies an electronic monitoring system9 in a given area, but the Customer only handles the data

It complied more than two months after it started on March 5, 2021, so it is a requirement

the requirement of adequate information was not fulfilled either.

Based on the above, it can thus be established that the Customer was not present at the registered office and the available

one

based on information, there is currently no adequate information on camera data management a

for employees working at the site (a total of 6 people during the examined period).

Based on the above, the Authority determined that the Customer violated the general data protection

paragraphs (1)-(2) of Article 13 of the Decree, and therefore called for legal compliance

to prepare a data protection information sheet.

5. Findings related to the applied sanction.

The Authority has examined what type of sanction it intends to apply to the Application

due to the revealed violations and whether it is justified to impose a data protection fine against him. E

in the scope of the Authority, Article 83 (2) of the General Data Protection Regulation and Infotv. 75/A. §-the

based on Infotv. § 61, paragraph (5), was considered by all the relevant parties of the case

circumstances and established that in the case of the violation discovered during this procedure, the Customer

9 See: The European Data Protection Board 3/2019. guideline no. personal data with video devices

about treatment, 28-29. She.

Online: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_hu.pdf

a warning and a warning in itself is not a sufficiently proportionate and dissuasive sanction,

therefore, the imposition of the fine is justified.

In establishing the necessity of imposing a fine, the Authority considered the violations

aggravating and mitigating circumstances as follows:

Aggravating circumstances:

- Unlawful camera data management and insufficient information at the investigated headquarters a

based on available data, it exists from March 5, 2021 until today. [general

Article 83 (2) point a) of the Data Protection Regulation]

- The Authority became aware of the data management based on a notification of public interest. The public interest

previously indicated to the notifying Customer the unlawful nature of the data management, in connection with which

however, the Customer did not take any action. [Article 83 (2) of the General Data Protection Regulation

point h)]

- When determining the amount of the fine, the Authority took into account that a

Violations of fundamental rights committed by the respondent are Article 83 of the General Data Protection Regulation

(5) to the higher maximum fine category

belonging to

are considered a violation of law.

Extenuating circumstances:

- Unlawful camera surveillance and lack of information are the investigated data management

only affected a narrow group of people (a total of 6 employees). [general

Article 83 (2) point a) of the Data Protection Regulation]

- Images transmitted by only two cameras ("office-customer waiting room" and "kitchen") can be on the site

suitable for unjustified surveillance of employees. [83 of the General Data Protection Regulation.

Article (2) point a)]

- During the procedure, the Authority did not come to the attention of any information that would indicate

that the affected parties would have suffered any specific disadvantage or damage as a result of the infringement.

[General Data Protection Regulation Article 83 (2) point a)]

- There was no circumstance that the circumstances of the data management were unlawful

during its formation, the Client would have been guided by intent, so only on his part

negligence can be established [General Data Protection Regulation Article 83 (2) b) and

points d)]

- The Authority took into account that the Client had not previously established the

violation of the law related to the management of personal data. [83 of the General Data Protection Regulation.

Article (2) point (e)]

Other circumstances taken into account:

- The Authority was also aware that the Client cooperated in everything

With authority during the investigation of the case, even though this behavior - because of the law

did not comply with obligations

as a circumstance. [general data protection regulation Article 83 (2) point f)]

too - he did not rate it specifically mitigating

The Authority is responsible for general data protection when making a decision on the legal consequences

did not consider points c), g), i), j) and k) of Article 83 (2) of the Decree to be relevant.

When determining the amount of the fine, the Authority took into account that the Authority is the Client

on the basis of the statement given at his invitation in the business year between January 1, 2021 and December 31, 2021

It had a net sales revenue of HUF […], i.e. HUF […]. In determining the fine, the violation

considering the period of its existence, the Authority took into account the 2021 business year. Above

based on this, the amount of the fine imposed is proportional to the severity of the violation and cannot be considered

excessive.

The Authority is Infotv. Based on § 61, paragraph (2), point c) of the decision, Customer identifier

ordered the disclosure of his data by masking it, as it does not affect him

a wide range of people.

ARC. 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 Akr. § 112, and § 116, paragraph (1), and § 114, paragraph (1) with the decision

on the other hand, there is room for legal redress through a public 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. § 13, subsection

(3) a)

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

Based on point b), legal representation is mandatory in a lawsuit within the jurisdiction of the court. The Kp. Section 39

(6) of the submission of the claim for the administrative act to take effect

does not have a deferral effect.

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 on the possibility of a request to hold a hearing in Kp. Paragraphs (1)-(2) of § 77

is based on.

The administrative lawsuit

law

(hereinafter: Itv.) 45/A. Section (1) defines. It is from the advance payment of the fee

Itv. Paragraph (1) of § 59 and point h) of § 62 (1) exempt the party initiating the procedure.

The Akr. According to § 132, if the obligee does not comply with the obligation contained in the final decision of the authority

fulfilled, it is enforceable. The Authority's decision in Art. according to § 82, paragraph (1) with the communication

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

XCIII of 1990 on fees.

the amount of his fee is

19

does not provide otherwise - it is ordered by the decision-making authority. The Akr. Pursuant to § 134 of

execution - if

law, government decree or local in the case of municipal authorities

the municipal decree does not provide otherwise - it is carried out by the state tax authority. Infotv.

Pursuant to § 60, paragraph (7), a specified action included in the Authority's decision

to carry out, for specific behavior,

obligation to

regarding the implementation of the decision, the Authority undertakes.

Budapest, March 29, 2022.

toleration or cessation

Dr. Attila Péterfalvi

president

c. professor

20