Case number: NAIH-963-10/2022. Subject: ex officio data protection

History: NAIH-7432/2021.

official procedure, fine

DECISION

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

Siófok Joint Local Government Office (headquarters: 8600 Siófok, Fő tér 1., hereinafter:

Customer 1) and the Siófok Police Department (headquarters: 8600 Siófok, Sió utca 12-20, the

hereinafter: Regarding Customer 2), for facial recognition in the administrative area of Siófok

regarding the operation of a surveillance system in public spaces that includes cameras

in official data protection proceedings initiated ex officio, in which the client was involved

Techno-Tel Telecommunications and IT, Contractor and Service Provider Limited Liability Company

Company (headquarters: 8600 Siófok, Bajcsy-Zsilinszky út 212, hereinafter: Customer 3) the

makes the following decisions:

I. The Authority

1. establishes that Customer 1 and Customer 2 are

was violated during data processing

about law and that

CXII of 2011 on freedom of information. Act (hereinafter: Infotv.) 25/B. § (1)

paragraph, 25/F. § (1) point d), 25/F. § (4) and 25/I. § (3)

points c) and e) of paragraph ;

information self-determination

2. orders the final decision with the publication of the identification data of the data controller

disclosure.

II. finds that Customer 3 has violated Infotv. 25/D. Section (3) point a) and e

due to infringement

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

data protection fine

obliged to pay.

The deadline for initiating a court review of the fine

collection of centralized revenues by the Authority within 15 days of its expiry

target settlement HUF account (10032000-01040425-00000000 Centralized collection

account IBAN: HU83 1003 2000 0104 0425 0000 0000) must be paid. The amount

upon transfer, NAIH-963/2022. FINE. number must be referred to.

If Customer 3 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

corresponds to the central bank base rate valid on the first day of the calendar semester affected by the delay

yes. The late fee is settled by the Authority for the purpose of collecting centralized revenues

……

1055 Budapest

Falk Miksa utca 9-11

ugyfelszolgalat@naih.hu

www.naih.hu

Phone: +36 1 391-1400

Fax: +36 1 391-1410

forint account (10032000-01040425-00000000 Centralized direct debit account)

to pay. In the event of non-payment of the fine and late fee, the Authority orders a

the execution of the decision, the fine and the late fee. The fine and late fee

collection of taxes is carried out by the National Tax and Customs Office.

During the official procedure, no procedural costs were incurred, therefore, no costs were incurred

was provided by the Authority.

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

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

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

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

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

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

representation is mandatory.

JUSTIFICATION

I. Facts, history

The Authority learned from press reports that Siófok City Municipality is using facial recognition

requires a camera system of 39 cameras enhanced with capable artificial intelligence

to be built on the Petőfi promenade in order to monitor the public area. Because for facial recognition

the operation of capable systems raises many data protection concerns, the Authority is Infotv.

51/A. (1) of § NAIH-5481/2021. launched an investigation, which

asked the Municipality of Siófok for clarification on the details of data management,

also requested to send more documents. The Municipality of Siófok City is the Authority

the requested documents in his response to your request - although to send them

referred to - did not make it available to the Authority.

According to this mayor's answer, in the area of the city of Siófok, starting from 2014, the public

LXIII of 1999 on supervision Act (hereinafter: Kftv.) on the basis of Section 7, Paragraph (3).

a public camera system was installed, which is operated by Customer 1's organization

City Guard operating as a unit (hereinafter: City Guard). The City Guard and Customer 2

cooperation on crime prevention and maintaining public safety has developed between

within the framework of which Customer 2 contributed to the camera system that started in 2020

continuously participated in its development and in the preparation of calls for tenders. Siófok

On April 18, 2021, the City Municipality issued a call for tenders

"In the framework of the modernization of the camera system of the Municipality of Siófok, cameras,

on the subject of acquisition of assets" for three economic companies. The bidding process

as a result, the City of Siófok concluded a sales contract on April 29, 2021

Municipality with Video-Data Kft., on the basis of which, on May 15, 2021, the

The dismantling of the old cameras on the Petőfi promenade in Siófok took place on June 15, 2021

installation of newly acquired cameras.

The test operation also took place on June 15, 2021, and the public space inspectors and

for the training of police officers, but this did not extend to (using the words of Customer 1)

to use the face detection function.

In his reply, the mayor emphatically emphasized that although the purchased cameras

have a face detection function, but it has not been activated. He recorded that

according to the preliminary impact assessment prepared by the data controller, artificial intelligence

would be attended by those involved

regarding his rights. This impact assessment

use with high risk

as a result, to initiate - prior to the use of artificial intelligence

the data controller at the Authority wanted Infotv. 25/H. conducting the preliminary procedure according to §.

According to the answer, the justification for the use of artificial intelligence stems from

that during the summer and especially on weekends, in the evening hours, there are many - thousands of -

people visit the entertainment venues on the Petőfi Promenade. All this comes with the

a drastic increase in the number of crimes and violations. The artificial

the use of a camera system equipped with intelligence would become much more effective

prevention of crimes/violations and crimes

detection.

The fact that the perpetrator disappears in the crowd regularly causes problems for the investigating authority,

all of this could be eliminated by using the new technology. The camera footage

looking back can also take several days, while artificial intelligence

this time could be shortened significantly.

According to the answer, the artificial intelligence - if it is turned on - is the following

would work according to:

The camera detects the faces of the people appearing in the recording; the recordings are closed IT

are stored on recorders installed in the system, which are overwritten every 30 days at the latest. The

when using face detection, separate so-called also thumbnails, which

are transferred to the system's video management server machine (DSS Server) and a dedicated one

They are stored on HDD. All this allows the operator to measure

perform a quick search from the video management client machine (DSS Client).

among stored thumbnails. This system is not connected to any database, that is

database is not transmitted, only the system stores it. If the concerned

I would follow his movement, so the marked face with the face in the system's database

would resemble

to start

human intervention is definitely required.

Operated by the data controller

camera system is not connected by Nemzeti Infokommunikációs Szolgáltató Zrt

done with data storage.

According to the answer, the purpose of data management is also Ktftv. Based on Section 7 (3) a

maintenance of public safety, crime prevention, measures and possible violations of law

documented recording, as well as the use of the recordings in connection with the infringement

in initiated proceedings.

The answer also addresses the fact that the data controller prepared an interest assessment test, in which it

established that the application of artificial intelligence would be proportionate to the desired goal

purpose, taking into account that only in a specific area of the city and defined

period it would be applied.

The answer records that the camera system was installed by Infotv. Section 5 (1) point a) and Ktftv.

It is operated by the City Guard (supervision of public areas) based on § 1 and § 7 (3). The

according to the point of view of the data controller, the legal basis for the use of the face detection system is Infotv.

Section 5 (2) point b) and Ktftv. § 1 and subsection (3) of § 7.

Although the answer refers to attachments and documentation, they were not sent

beer.

According to the opinion of the Authority, the case that is the subject of the investigation is within the framework of an

investigation procedure

could not be clarified, therefore Infotv. Section 55 (1) point ab) and Section 60 (1)

on the basis of paragraph, closed the investigation procedure and initiated an official procedure ex officio

NAIH-6212/2021 against Siófok City Municipality. number.

together. The artificial

of its application

intelligence

3

possessors

created - which you attached to your answer

As part of the official data protection procedure, the Authority invited Siófok to make a statement

City Municipality, on whose behalf the Mayor of Siófok answered August 2021

on the 3rd day. In this and earlier, in the answer given in the framework of the investigation procedure, and its

two camera rooms and an operator's room were marked in its annexes. One of them

such a room is the camera room of the City Guard (8600 Siófok, Kálmán Imre sétány no. 4), while the

another room was created at the headquarters of Customer 2. Pertaining to Customer 1

city of Siófok based on the data management information sheet - which was attached to the answer

The data controller of public cameras placed in the area is the City Guard, which is the clerk

represents; and Siófok on the Organizational and Operational Regulations of the Local Government

9/2013 of the Board of Representatives of the City Self-Government. (III.3.) municipal decree (a

hereinafter: Regulation) according to Section 5 (5), the official organization of the representative body a

Siófoki Joint Local Government Office, located in the Siófoki Joint Local Government Office

Office City Guard camera room. According to § 46 of the Regulation, Customer 1 is a legal person, independently

operating and managing budget body. According to Annex No. 3 of the Regulation a

City Guard Client 1 organizational unit within the Authority Department.

The Response states that the Municipality of the City of Siófok and Client 1 and the Counties of Somogy

Cooperation agreement between police headquarters in 2013 (hereinafter:

Cooperation Agreement) came

also – which

lays the foundation for cooperation with regard to cameras in public areas. According to this, the summer

period in the presence of public area inspectors in the police building - closed,

with an entry permit only

accessible to - observer

the head of the police department is present in the room, who detects the incident

informs the police on the spot. If the police - the procedure

to conduct it - you need footage recorded by the public area camera system, so that's it

after submitting a written request - inquiry - it will be handed over to the police a

Ltd. in accordance with its provisions.

According to the response, the data controller established that as a result of the data protection impact assessment

and that since biometric data would be processed, it would entail a high risk

regarding the rights of the data subjects, this is why the data controller decided not to use the cameras

this function, but wanted to initiate a preliminary consultation with the Authority. The

the data controller would decide to set up the application in a policy,

that it could only be in the area of the Petőfi promenade and only on weekends during the summer

apply, elsewhere and not elsewhere; the function is performed by the currently serving public space-

supervisor would activate it.

The answer details the operation of the facial recognition application, which is consistent

marks as face detection.

The documents of the bidding procedure requested by the Authority, as well as the Video-

A copy of the contract concluded with Data Kft. Also attached is the data protection

impact assessments, one of which is conducted without artificial intelligence

refers to data management, and the other is to the use of artificial intelligence

for data management. Also attached to the answer was a copy of the interest assessment test, a

network topology of the camera system, construction plan of the infrastructure of the camera system, a

Document regarding the location of the Petőfi Promenade cameras, as well as the city of Siófok

on the designation of the location of public area video recorders located in the public administration area

solo presentation, the public administration of the city of Siófok

cameras located in the area

on the change of its number, 145/2013 on the amendment of the municipal decision

submission, and public land located in the administrative area of the city of Siófok

the proposal on the designation of the placement of video recorders and the one made on the basis of them

copy of representative body resolutions.

without intelligence

Based on the content of the attached documents, the following should be highlighted:

Customer 1 Data management related to public cameras located in the City of Siófok

according to its information, the range of personal data processed is monitored by the camera in public areas

image of persons entering the area (image and video recording). The purpose of data management is a

CLXXXIX of 2011 on Hungarian local governments. Act § 13 (1)

paragraph 17 and § 17; the Ktftv. public safety according to § 1, § 7, paragraph (3),

crime prevention goal and the protection of municipal and community property. The

the legal basis for data management is Infotv. Section 5 (1) point a) and Ktftv. § 1 and § 7

Paragraph (3). The footage recorded by cameras in public areas, after recording, Ktftv. Section 7

It will be deleted after the time specified in point b) of paragraph (7). Customer as data processor

3 was determined.

The Cooperation Agreement regarding the public area camera system

does not contain a provision.

The artificial

data protection for data management

according to the impact assessment, the purpose of data management is sufficiently defined and legal, taking into account

that the data management is carried out by Ktftv. prescribe; data management is proportional to the achievement of the goal

and the goal

necessary for its effective implementation.

Data protection impact assessment for data management with artificial intelligence

according to Infotv, the legal basis for data management. Section 5 (1) point b), as well as Ktftv.

§ 1 and § 7 (3); the data protection officer recommends the artificial

not using intelligence, taking into account that biometric data management

is happening, and in his opinion it cannot be established beyond doubt that it is

the use of data management is proportionate to the goal to be achieved. Noting that it is

during data processing, biometric data would also be processed, and data processing is high

with risk

regarding his rights and freedoms, the data controller a

prior to the application of artificial intelligence, the Authority initiates in advance

consultation procedure.

According to the balance of interests test, data processing is indeed limited by the data subjects

his constitutional fundamental right to the protection of his personal data, however, the limitation is one

widely recognized interest in society, for the sake of public safety and crime prevention

happens; intended to be used by the data controller

(specified only

period, data processing would only take place in a specific area) they make the

restriction.

On August 26, 2021, the Authority ordered an on-site inspection of Customer 1 and Customer 2

at its headquarters, as well as in the camera room of the City Guard.

Dr. was present at the site inspection held at the headquarters of Customer 1. Clerk József Sárközy, dr.

Nikoletta Kovács data protection officer, ……. public area supervisor, as well as

…….. as a representative of Customer 3 and …….. as an employee of Customer 3.

As part of the on-site inspection, Dr. Nikoletta Kovács is the data protection officer acting for the Authority

to a member's question, he stated that the camera room of the public area camera system is Customer 2

located at its headquarters; The City Guard is considered to be the data manager, servers are in several locations

are located, for example, at the headquarters of Client 1 and Client 2, as well as in the camera room of the City Guard

(Imre Kálmán promenade). He also submitted that the camera surveillance is only for Customer 2

in his building by public area inspectors, however, during the summer, by the police

its professional members are also present; It is for cooperation with customer 2

would be attended by those involved

provisions

function is available. Data transmission is secured via optical cable

It is based on a Cooperation Agreement. He also said that the camera system

its face detection function does not work, nor has it been tested. He submitted that the

relevant data management information is available on the city's website in Hungarian, the cameras

according to geolocation, they are indicated with their bearing angle. If the face detection function

would be used, the data protection policy would be amended, or specific

boards

would also be posted. Data requests from the authorities are documented, a

In all cases, the police issue a confiscation decision and report. Customer 3 a

provides technical support in relation to the management of recordings.

…… as a representative of Customer 3 submitted that the data storage is exclusively for Customer 1

building, while video is displayed in the camera room of Customer 2 and the City Guard

there's an opportunity for; 2 workstations are set up at both locations, from which the DSS

system

is happening.

He said that previously, within the framework of independent projects, the devices of several manufacturers were placed in the

to the city starting in 2013, however, it became necessary to purchase a platform that

which is capable of managing the data of all camera systems, thus the choice was made

For Dahua cameras. At the same time, the possibility of face detection was not expected, although the

a camera system can also do this; images of all cameras operating in the city area a

accessible from workstations in a unified system. 38 Dahua on the Petőfi promenade in Siófok

cameras were built, including 14 PTZ and 24 fixed cameras. He presented that it is

prior technical intervention would be required to use the face detection function a

by the manufacturer and the operator.

……. according to the statement of the public space inspector in the City Guard's camera room

monitoring takes place throughout the year, but not permanently, but periodically.

He submitted that public area supervisors enter the system with the same login; individually

it is not recorded who entered, the number of entrants can be narrowed down based on the service schedule.

Acting members of the Authority visited the server room where two IVSS servers were located

for placement that have artificial intelligence.

Client 1 handed over to the acting members of the Authority who are authorized to enter the server room

roster.

The

volt

……., dr. Nikoletta Kovács as Customer 1 data protection

official, …….. public space inspector,

also …… and

…….. From Customer 3.

The acting members of the Authority established that the operator's room and the server room are physical

protected by security.

…….. presented that to the professional staff of the Client 2

police officers involved in monitoring the camera images; to the operator's room

entry is possible with a key in the custody of the shift commander, which can be collected

are documented. The key can only be used by professional members of the police and public area

may be taken over by supervisors. Client 3's employees can only move around with a police escort

in a building. For camera surveillance not continuously, but in justified cases, like this

especially in the case of a city event, event or suspicion of a more serious crime

will take place. Client 2 professional staff members only live video monitoring and current

you can document the direct history of the event in a few minutes

way. In addition to all this, the saved camera footage can be seized upon request of the City Guard

it is acquired by decision of Customer 2. According to his statement, face recognition or face detection function

cannot be used by the police.

at its headquarters

on-site

review

Customer

held

present

At the time of the Authority's on-site inspection, the police are professional in the operator's room

member of the staff conducted an observation.

A member of the Authority with IT expertise examined the subject of the investigation

the central DSS console of the system, whose administrator interface is a web browser

can be accessed using The data required for access is provided by Customer 3 as a data processor

his colleague, …… knew and entered with administrator rights.

The acting member of the Authority established that Police, Technotel, Operator and Administrator

roles were set, as well as Police, City Guard, Technotel and System users

was recorded.

From a single live and usable log file, it was possible to determine that system

delete, create and modify roles and users with administrator rights

occurred on August 26, 2021 between 1:13 p.m. and 1:22 p.m. Deleted

usernames: Laci, user; deleted roles: Glaci, Nezo; added role: police;

while modified user: Police, Technotel.

The system was not suitable for examining other log files.

3 employees of the customer, …….., stated that they had already been notified of the logging out several times

fault to Dahua as the manufacturer.

The above were not disputed by the representatives of the clients present on the spot, according to the minutes

no comments or other proposed amendments were made regarding its content.

Based on the examination of the license file, it could be determined that it was purchased for 284 channels

of the license, 274 video channels were active and face recognition could be activated for 69 channels

0 channels were active from the license.

From the system status page, it could be determined that 33 devices were online and 2 were offline

in system; also 2 users were online and 2 offline; there were also 17 services

online.

1365 GB of the system's 1823 GB storage capacity was in use during the on-site inspection

at the time.

The acting member of the Authority took a photo of all these circumstances.

In response to a question, the inspector of public spaces said that it was about the registration of rights

he does not know, only about what is available to the police, and there is also no log data

at the disposal of the City Guard.

The document "Statement on the use of the camera room" is attached to the minutes,

which includes the time of use of the operator's room and the occupants

designation, as well as recording whether a seizure has taken place. These documents

according to his testimony, between August 20, 2020 and August 26, 2021, only

In 19 cases, the operator's room was used, and in the vast majority of cases it was not

a public area inspector was shown alongside the policeman. Furthermore, the cases are also significant

part, approx. in half, specific criminal and violation cases were also indicated

as a goal.

The acting members of the Authority established during the inspection of the City Guard's camera room,

that the camera room consists of one room, there are two workstations from which

the public area camera system

available after entering a password;

username and

the camera room opens from the Kálmán Imre promenade in Siófok, the physical security is one, directly

means the door opening from the street; no one was in the camera room during the on-site inspection

at the time, it was empty.

Undoubtedly based on the data obtained in the framework of the official data protection procedure

it has been established that the Municipality of Siófok City is not a data controller,

nor to a common data controller and data processor. In view of the above, the City of Siófok

NAIH-6212/2021 was filed against the municipality as a client. data protection
official procedure was terminated by the Authority. However, it is also capable of facial recognition
surveillance system expanded with cameras, and the data management implemented with it is official
investigation in the procedure was still necessary and with Customer 1 and Customer 2
against NAIH-7432/2021. initiated a data protection official procedure at
Authority in which NAIH-6212/2021. used the documents of the proceedings.
The legal status of customer 1 is based on the fact that Ktftv. public area designated as data manager by
supervision - in this case the organizational unit of the City Guard - Client 1. Customer 2 customer
the basis of his legal status is that he participates in surveillance with the camera system, which
the data management system is performed with the device elements at its own headquarters, thus data management
conducts activities.
As part of clarifying the facts, the Authority invited Client 1 to make a statement. Customer 1
according to his answer, he did not issue an instruction to change the roles, it was done by Customer 3
performed voluntarily by your employee; also attached by Customer 3 regarding this
statement that the case was investigated and the necessary steps were taken
against the data processor. In his answer, he explained that the police are professional staff
members used the camera system in the presence of city guards (public space inspectors).
Attached with the errors in the log files provided in writing by Dahua Technology Hungary Kft
related electronic response dated November 5, 2020. He also stated in his reply,
to investigate the case in the news published on the city's website on June 10, 2021
no artificial intelligence was used during; simultaneously sent by Customer 2 reservation
decision by which the relevant recording was seized.
In the context of clarifying the facts, the Authority contacted Customer 2, which in its response
recorded that on the DSS terminal located in the operator's room for Customer 2's files
none of its members have deleted, modified or created roles and users.
According to his statement, the only professional members of the police are city guards (public

supervisor)

had access to the data that can be extracted from the camera system,

considering that Customer 1 is considered a data controller; at the same time, he also recorded that

however, the police perform joint data management when using the camera system

necessary for all procedures to acquire the data (recording) in an official procedure,

contact the data controller for its use and reserve the data; the new policy

role provides a limited opportunity to use the system, however, since it was set up

the practice of asking the City Guard for help in extracting the data has remained.

According to his statement, not to detect the crime committed on June 10, 2021

they used artificial intelligence; sent him at the same time for this crime

confiscation decision issued in the proceeding. According to his statement, July 12, 2021 and

Operator observation took place in the operator's room between August 26, 2021.

"Statement on the use of the camera room" document available to the Authority

however, it does not contain an entry for this period.

The Authority contacted Dahua Technology Hungary Kft. in order to clarify the facts.

In its response, Dahua Technology Hungary Kft. explained that Dahua is involved in the project

only provided products, they did not participate in the procurement contract;

in his presence

also that some

know how to activate the

In 2020 and 2021, he sold the closed-chain monitoring connected to the project

products to Hungarian distributors. He explained it

their products

support face detection/face recognition function (FD/FR function) which is default

is turned off and must be activated manually if required by end users; that

a person who has this kind of training or who previously operated the

devices,

function; admin for all of that

authorization is required.

Based on the obtained data, it could be established that Customer 3 is the data management system

provides technical support for its use, this official case directly affects your right, it is legitimate

interest, therefore involving him as a client and inviting him to make a statement is NAIH-7432-

8/2021. It took place on November 30, 2021 in Order No.

According to the available data, Client 3 is an employee of the Authority's on-site procedure

at the time - without instructions - the Customer deleted or created roles and users

2 on the DSS terminal located in the operator's room.

According to the relevant statement of Customer 3, there was a communication misunderstanding by the Authority

part of the procedure, the so-called regarding log files; because in the DSS Pro system the

concerning activity

log files (Client operation log and the Web manager

operation log) - as opposed to the "system log" - they have not experienced

malfunction. During the on-site inspection, Customer 3's employee is the "System log".

He made a statement regarding the system log. Given that they have not experienced a fault

operation in relation to the Client operation log and the Web Manager operation log, thus

no report was prepared, no action was initiated. According to Customer 3's point of view

the Authority's belief that the user activity log is incorrect

(Web manager/Client operation log) would work abnormally; furthermore, that the system log

(System log) does not contain entries and is not considered an error. He further explains that a

NAIH-6212-6/2021. in the case of Annex No. 3 of Protocol No. 3, the period filter is only

was set for a one-day time interval (from 08.26.2021 to 08.26.2021). Customer 3

voiced his incomprehension

in terms of what the Authority can train on it

the basis of its assumption that the logging of user interventions is inadequate.

In order to prove everything, he attached for the period following the site inspection the

Web operator operation log November 21 and November 27, 2021, and the Client

operation log data between November 20 and November 26, 2021. At the same time

stated that as operators they are not aware that the system is activity

its logging would not or would work incorrectly, so no action was taken. He further stated that

the activity logging time interval is currently the factory-set period of 30 days,

according to this, user activities in the last 30 days can be considered

and in the event log; if the Authority "requires" this setting to be modified, so

asks to determine the duration.

To support the claims of Customer 3, it was sent by the Customer's operation log and the Web Manager

operational log screenshot with the comment that they work perfectly.

Sent by the City of Siófok, dated September 24, 2020, together with Customer 3's response

Municipality as customer/data manager and Customer 3 as contractor/data processor

"Flat-rate maintenance and data processing contract" concluded between

Contract).

Customer 1 sent a statement with the same content as Customer 3's answer to the Authority in 2021.

on December 21 regarding the log files.

II. Applicable legal provisions

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

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

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

Infotv. According to § 3. 3, special data in special categories of personal data

all data related to racial or ethnic origin, political opinion, religion or

personal data referring to religious beliefs or trade union membership, as well as

genetic data, biometric data aimed at unique identification of natural persons,

health data and sexual life of natural persons or sexual

personal data regarding your orientation.

Infotv. § 3. 3b. point, biometric data is a natural person's physical,

obtained by specific technical procedures related to its physiological or behavioral characteristics

personal data that enables or confirms the unique nature of the natural person

identification, such as facial image or dactyloscopic data.

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

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

at bodies authorized to conduct and detect crimes, and a

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

personal data on criminal record.

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

unincorporated organization who or which - in law you are

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

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

used tool) makes and implements relevant decisions, or is

performed with a data processor.

Infotv. § 3.9a. point, a joint data controller is a data controller who or which -

within the framework defined by law or a mandatory legal act of the European Union - that

determines the purposes and means of data management jointly with one or more other data controllers,

one or more decisions regarding data management (including the device used).

jointly with another data controller and carried out or carried out by it

with a data processor.

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

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

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

transmission, disclosure, coordination or connection, blocking,

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

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

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

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

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

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

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

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

to participate in the procedure,

also in the criminal procedure or violation

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

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

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

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

purpose) data management.

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

making it available to

Infotv. According to point 17 of § 3, data processing is on behalf of the data controller

set of data processing operations performed by a data processor acting on the basis of its provision.

Infotv. Pursuant to Section 3.18, a data processor is a natural or legal person,

or an organization without legal personality, who or which - in law you are

within the framework and under the conditions specified in the binding legal act of the European Union - that

processes personal data on behalf of or at the request of a data controller;

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

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

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

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

pursuant to section (2) only personal data that is

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

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

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

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

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

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

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

it is absolutely necessary and personal data is concerned

to perform its tasks

expressly contributed to its treatment,

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

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

necessary to prevent or prevent imminent danger and thereby

you are cute

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

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

cute.

(2) Special data

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

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

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

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

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

11

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

law, international treaty or a binding legal act of the European Union otherwise not

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

apply.

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

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

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

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

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

review and amend accordingly if necessary.

Infotv. 25/B. According to § (1), if a law, an international treaty or the European

The binding legal act of the Union is related to the data management carried out by joint data controllers

by fulfilling obligations, especially by asserting the rights of the data subject, as well as

the distribution of their responsibility for failure to fulfill these obligations

does not or does not fully define it - by the legal obligations governing them

to a non-regulated extent - the joint data controllers are established in writing between them and

determined in a made public agreement.

Infotv. 25/C. Pursuant to § (1), as a data processor, you are only such a person

organization

who or which provides adequate guarantees for data management may act

technical and suitable for ensuring its legality and the protection of the rights of those concerned

to implement organizational measures. These guarantees start the data management

the data processor confirms it to the data controller beforehand.

Infotv. 25/D. pursuant to paragraph (1) of § between the data manager and the data processor

the detailed content of the legal relationship in this law, as well as the mandatory legal provisions of the European Union

or the data controller and the data processor within the framework defined in act

written contract between - including the contract created electronically

- Define. For the legality of the instructions given by the data controller to the data processor

the data controller is responsible.

(3) It must be stipulated in the law or contract specified in paragraph (1).

in particular on the obligation of the data processor to

a) in the course of his activity, he acts solely on the basis of the written instructions of the data controller,

b) in the course of its activities, it ensures that it is for the personal data concerned

persons entitled to access - if appropriate confidentiality based on law

they are otherwise not under the scope of the obligation - the personal data they have learned

undertake a confidentiality obligation regarding

c) in the course of its activities, the data controller is assisted by all appropriate means

to facilitate the enforcement of your rights, in order to fulfill your obligations in this regard,

d) at the choice of the data controller, the completion of the data management operations carried out by him

after - if the law does not provide otherwise - or cancel its activity immediately

personal data learned during the process, or forwards them to the data controller and it

deletes the existing copies after

e) the data controller

provides everything

data processor

required for verification and

regarding its use

yogi

information that is

compliance with regulations

12

f) an additional data processor only if the conditions specified in this law are fulfilled

takes

Infotv. 25/F. Pursuant to paragraph (1) of § § 1, the personal data has been processed electronically

for the purpose of verifying the legality of data management operations, the data controller and

data processor in an automated data management system (hereinafter: electronic diary)

records

a) defining the range of personal data affected by the data management operation,

b) the purpose and reason for the data processing operation,

c) the exact date of the data management operation,

d) designation of the person performing the data management operation,

e) in the case of transmission of personal data, the recipient of the data transmission.

(2) The data recorded in the electronic log are solely for the legality of data management

control, enforcement of data security requirements,

and criminal proceedings

can be known and used for the purpose of conducting

(3) For the electronic diary, the Authority, and for the purpose specified in paragraph (2).

for persons and organizations engaged in legally defined activities - those

at your request for this purpose - the data manager and the data processor provide access, from it

transmits data to them.

stored personal data

unauthorized reading, copying, modification or

(4) In the data controller and data processor register, as well as in the electronic diary

recorded data must be kept for ten years after the deletion of the processed data.

Infotv. 25/I. According to paragraph (3) of the data controller, it is within the scope of its activities

data processor ensures with the measures specified in paragraph (1).

a) the tools used for data management (hereinafter: data management system) are unauthorized

denial of access by persons,

b) data carriers

preventing its removal,

c) unauthorized entry of personal data into the data management system, as well as

in that

unauthorized access or modification

preventing its deletion,

d) data management systems by unauthorized persons, via data transmission equipment

preventing the use of

e) that the persons authorized to use the data management system are only the access

have access to personal data specified in the permit,

f) that it can be checked and established that the personal data is transmitted

via equipment to which addressee it was or may be forwarded, or issued or

can provide

g) that it can be subsequently checked and determined which personal data,

at what time, who entered it into the data management system,

h) personal data during their transmission or during the transport of the data carrier

by

deletion

preventing,

i) that the data management system can be restored in the event of a malfunction, as well as

unauthorized access, copying, or modification

signal,

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

j) that the data management system is functional, about errors occurring during its operation

a report should be prepared, and stored personal data will not be stored due to incorrect operation of the system

can be changed.

Kftv. According to paragraph (3) of § 7, supervision in public areas, public safety, or

for the purpose of crime prevention, you can place a video recorder in a way that is obvious to anyone

and you can record. About the placement of the imager and what was observed with the imager

the representative body decides on the designation of a public area for submission to the supervision.

(4) The video recorder is operated and managed by the supervision. The supervision of the placement of video recorders

and informs the police about the public area observed by the videographers, as well as these

data on the website of the mayor's office of the municipality operating the supervision

publishes it.

(5) In a way that facilitates the information of persons entering the area monitored by the videographer

attention getter

a description of the location of the image recorders must be placed, that is

about the fact of data management.

XXXIV of 1994 on the Police. Act (hereinafter: Rtv.) § 42. (2) paragraph

according to the police in public areas, where public safety, crime prevention and law enforcement

a video recorder that is verifiably necessary for the purpose, in a way that is obvious to anyone

you can place and record.

The

law

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

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

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

deadline one hundred and fifty days.

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

shall be applied with the deviations specified in

The Akr. On the basis of § 103, paragraph (1), in the official procedure initiated ex officio, the Ákr

the provisions of the Ákr. VII. contained in chapter

must be applied with variations.

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,

according to paragraph (3) of the same §, the ex officio procedure is the first procedural act

begins on the day it is completed, the authority will notify the known client of its initiation.

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

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

in connection with operations, you may determine that personal data is being processed illegally

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

the

deletion or destruction,

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

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

data controller unlawfully refused, and may impose a fine.

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

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

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

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

blocking of illegally processed personal data,

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

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

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

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

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

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

brought in connection with his activity, or what happened

gravity of infringement a

justifies disclosure.

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

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

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

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

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

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

you can use it in your procedure.

In addition to the decision, the Ákr. Sections 80 and 81 shall apply.

III. Decision

The purpose of the Authority's procedure is the public camera system operating in the city of Siófok

was an investigation of data management, published in the press by the mayor of the city of Siófok

in view of his statement that the camera system capable of facial recognition is artificial

enhanced with cameras with intelligence. The facial recognition

function contingent

in addition to the examination of its application, the subject of the procedure was the public area "in itself".

with a camera system - without the use of a face recognition function - is possible

examination of data management.

III.1. Data management by the facial recognition function of the public area surveillance system

judgement

Regarding the camera surveillance of the public area, Kftv.

Paragraph (3) of § 7 allows that on public land, public safety or crime prevention

purpose, place a video recorder in a way that is obvious to anyone, and record

make; on which the representative body decides to submit to the supervision. By the same token

pursuant to section (4), the video recorder is operated and managed by the supervision; the

supervision of the location of the video recorders and the public area monitored by the video recorders

informs the police, as well as this information by the operator of public space supervision

it is also published on the website of the municipality's mayor's office.

For the police, Rtv. Paragraph (2) of § 42 ensures that the photographer - for anyone

placement and recording in an obviously perceptible manner, that is

in public areas, where it can be justified for public safety, crime prevention or law enforcement purposes

required.

Infotv. The concept of special data defined in point 3 of § 3 includes a

biometric data for the unique identification of natural persons.

Infotv is considered biometric data. According to point 3b) of § 3, a natural person

with specific technical procedures regarding its physical, physiological or behavioral characteristics

obtained personal data that enables or confirms the unique nature of the natural person

identification, such as facial image or dactyloscopic data.

According to the mayor's statement, the surveillance system is not connected to anything

database, the data is not transferred to another database, only the system

store them. If the movements of the affected person were to be followed, the marked face would be a

would compare it with facial images in the system's own database. According to the statement, the

system is not connected to the data storage provided by NISZ Zrt.

In terms of handling personal data, the Authority uses the camera system's facial recognition function (mentioned in the mayor's statement as a "face detection" function) - as written above in relation to its application, it states the following in general:

By applying the face recognition function - as referred to above - from a face image by executing a database operation based on a stored thumbnail, with the face image the marked person can be easily identified individually in further recordings. Since the system according to the declarations, it is not connected to other records (e.g. personal data and residential address register), therefore they cannot yet be naturally linked to the person concerned personal identification data. Regardless, the face image and the search based on it, or, as a result of hits, the selected person is the additional one included in the recordings separable from persons, actually uniquely identifiable, and subsequently it becomes easy to follow and observe the recordings stored in the system at a given time.

The system is capable of facial recognition in its own database through artificial intelligence search and the selected face image as personal data from further recordings selection is, by definition, biometric aimed at the unique identification of the given person means data management. All this is independent of whether you are natural personal identification data establishing the identity of the data subject by means of other personal identifiers this system alone cannot do it.

Artificial intelligence capable of facial recognition is carried out within the framework of a camera system use - based on the above and the legal provisions - clearly biometric data, thus resulting in the processing of special data.

During the investigation procedure prior to the Authority procedure, the mayor of the city of Siófok is the Authority in the reply sent to your inquiry with file number SFK/35304-2/2021, the camera system above mentioned its function as a face detection system, which is the legal basis for its use Infotv. § 5, paragraph (2) point b) and Ktftv. § 1 and § 7 (3) referred to.

Infotv. The definition of § 5 (2) point b) as a legal basis is obvious

incorrect; because according to this, special data can be processed if it is declared by law

is absolutely necessary and proportionate to the implementation of an international agreement, or it is

Enforcement of fundamental rights guaranteed by the Basic Law, and national security, a

for the prevention, detection or prosecution of crimes or national defense

in the interest of the law.

The Ktftv. Paragraph (3) of § 7, as well as Rtv. Provision (2) of § 42 - which on public land

the public area supervision and the police provide the opportunity to take pictures

for - creates a legal basis for processing personal data. The video recording takes place in a public area

these provisions regarding the possibility of placing and taking pictures

cannot be interpreted as simultaneously providing authorization for stricter data management

subject to conditions

belonging to biometric data requiring stricter guarantees, such as

to handle special data. The purpose of the legislator in creating these legal provisions

it is not possible to manage biometric data using facial recognition

was aimed at

term

technician

also face recognition

The Authority did not investigate in detail the issue that if Customer 1 and 2

available software would have been activated and applied, then biometric data

under what conditions the treatment would have taken place. This can only be examined then

would be possible if supported by evidence and under reconstructable conditions

this would have already taken place at the time of the on-site inspection or before

for data management.

In any case, however, the fact that the data controllers, the data processor and the person in question

the camera system based on consistent statements made by the camera system manufacturer
is equipped with artificial intelligence capable of face recognition (face detection), means
that within the scope of personal data, biometric, i.e. special data, can also be processed
capable camera system was built. However, the Authority is special in this case
did not establish the fact of data management.
Customer 1 repeatedly emphasized in his statements that the available software is not
face recognition, but face detection. The Authority does not wish to enter into a semantic debate
say goodbye to face recognition/face detection
regarding, since
according to his point of view, there is no substantial difference between the two definitions. For data management
the operation of an available camera system equipped with artificial intelligence
during - although not connected to a database - but from recordings and thumbnails
creates a database by itself and matches the search result to it. It should be noted
otherwise, the program itself
identifies all of this as a function
(Annex 4 of minutes No. NAIH/2021/6212/6/2021).
During the current procedure of the Authority - the client's statement and the on-site inspection a
based on the small amount of data extracted from the camera system at the time of the inspection - that a
for determination
intelligence
it has not been used by customers so far.
At the same time, the Authority draws the attention of Customer 1, Customer 2 and Customer 3 that currently the
Current legislation does not allow a public space monitor handling biometric data
operation of the system in Hungary.
The Authority wishes to refer Infotv. principles, which apply during its procedures
check.

Infotv. Pointing to paragraph (2) of § 4, the Authority emphasizes that the necessity

proportionality

all

based on a detailed examination of its circumstances, it will be judged and enforced in the future as well.

Regardless of this, it should also be highlighted that it is in itself if it is provided by law

the legal basis of data processing, it does not even mean that the data processing is considered legal if

without regard to the requirements of necessity and proportionality. Personal data

within the scope of the management of biometric data as special data, the necessity and

assessment of proportionality requires particular care, since biometric data

management of the data subject's right to self-determination with personal data in itself

is severely restricted. They must be proportionate to this serious limitation

to be, and the goal achieved by data management must be proportionate to this.

It should be noted that Customer 1 attached to his reply received on December 21, 2021 the

The press release of the Metropolitan Prosecutor's Office, which is the commission of a terrorist act

reports on the prosecution related to its preparation, one of the places where it was committed

it would have been a promenade in Siófok. Customer 1 also wanted to support the fact that the promenade

outstanding in terms of law enforcement and crime prevention.

it turned out that it is artificial capable of facial recognition

requirement

enforcement

case by case,

case

the

17

The Authority does not dispute all of this, but at the same time – from the point of view of necessity and proportionality –

points out that in this case

also the law enforcement authorities in the preparatory course

they prevented crime without being placed on the boardwalk and artificial

a facial recognition camera system with intelligence would have been used. It appeared

also a notice on the website of the city of Siófok on June 10, 2021, according to which a

the police were able to identify Mártírok úti with the help of the promenade's camera system

railway barrier breaker. The present procedure clarified the details of this case, according to which the perpetrator

without the use of the facial recognition function, the recorded image recording by the police

by asking, a

public announcement

identified as a result.

III.2. Revealed during data management with the surveillance system,

deficiencies

police website

published

illegal

through

measures are applied,

III.2.1. Defining the role of the participants in data management

Based on the legal definition of the data controller, the quality of the data controller is defined as being a data controller

the one who independently or together with others determines the purpose of data management

makes decisions regarding data management (including the device used) and

executes it or has it executed by the data processor.

Decisions regarding data management include, for example, the determination that a

organization will perform data management. Likewise, decisions about whether a

which areas should be monitored with surveillance cameras, which camera system should be used,

during which period the data is processed, who is entitled to access the data, what kind

data security

whether they are used and exactly what kind

data processor in the field of activity. Furthermore, the decision regarding data management is itself

execution of data management operations and data controllers related to the exercise of data subject rights

fulfillment of obligations.

Customer 1's statement(s) included in the minutes and made available to the Authority

in documents,

and the city of Siófok

on the designation of the placement of public area video recorders located in the public administration area

in submission; of the number of video recorders placed in the administrative area of the city of Siófok

on its change, 145/2013 in a proposal to amend a local government decision;

also administrative of the city of Siófok

public area video recorders located in the area

contained in the proposal on the designation of its placement; as well as the data controller

system, its tools and conditions inspected on site by the acting members of the Authority

they certify that Customer 1 is clearly the data controller of the subject of the procedure

public space surveillance system.

Kftv. in accordance with its provisions, on the recommendation of the City Guard (public area supervision)

the municipality decided to start the surveillance system, i.e. the data management,

about its tools

about the replacement of certain elements of the system,

its development, expansion with additional cameras and other devices. carried out

or performed with the data processor - for data management, the surveillance system

commissioning

carrying out his duties,

City Guard (as the organizational unit of Customer 1) designated by law as data controller

perform data management operations, such as occasional viewing of recordings,

reviewing, saving, handing over to the bodies authorized to do so.

relevant decisions. THE

so the data management

or the existing one

public space supervision

in a prospectus;

18

logically

necessity

Although the relevant data management information, as well as the legal provisions and the

based on actual daily practice, clearly Client 1 (the City Guard as an organizational

unit) is the data controller (joint data controller), yet dated September 24, 2020

The contract was concluded by the Municipality of Siófok as data manager.

Statements made by customers and observed during the on-site inspection and in the minutes

recorded circumstances, as well as requested by the Authority and attached to the protocol

documents (such as the document called "Report on the use of the camera room")

it was also established that Customer 2 is also a data controller

the following regarding data management with the same surveillance camera system

Based on.

On the one hand, Customer 2 participated in the decision to expand the camera system

in such a way that the tools to be acquired during the expansion of the system contributed

selection, i.e. in the decision regarding data management tools.

On the other hand, Customer 2 carries out specific data management operations at its own headquarters for image recordings

through observation in an operated camera room. According to Customer 1, it is

Observation by customer 2 takes place with the participation of public area inspectors, however, a

Detected on site by authorities and sent to the camera room at Customer 2's headquarters

on the basis of entry documentation, the workstations in the police station in daily practice

on one of them, in most cases, the surveillance is carried out independently by a police officer belonging to Client 2's staff

performs. According to Customer 2's statement, the monitoring is not continuous, it is taking place in the city

specific events, events to be secured, other reasons are determined by the image recordings

looking back

goals

they can justify. Occasionally, to review the recordings in a short time interval

also performs a relevant data management operation if necessary. All of these

based on this, it can be said that Customer 2 decides when he finishes in the camera room

observation. Based on what is directly observed in the images, it can and does in any given case

police action. From a data management point of view, this means that there is a way to do without

actually use the information and data detected in the recordings to make the recording

you should request it separately from Customer 1. Statements made during the procedure and attached

according to documents, if Customer 2 does not directly interfere with the recordings

for the sake of, but further use as evidence for one of its proceedings

needs, he requests it from Customer 1 by means of a reservation.

It should be emphasized that for all these data management activities Rtv. taking pictures in public areas

provides a legal basis for Customer 2.

The role of joint data controller of Customer 2 is also supported by the fact that it is joint

data management

in an established camera room

data management system elements, tools and the building another

taking measures aimed at the physical security of the server in its premises, as well as

ensuring access to them - especially with regard to the public duties of Customer 2, public authorities

role and related security regulations and regulations -

available only to Customer 2.

Customer 2 allows entry to the operator's room in his building, or

supervises and protects with physical security. What happened there with administrative means

document it. The camera system for Customer 2 with the "Police" role, or user

accessible by name.

According to the facts established during the Authority's procedure, the data management of Customer 2 is currently a

for the data management operations presented above (monitoring of live images; short recordings

looking back at time intervals; on the basis of direct observation of the recordings

in the course of activity at Customer 2's headquarters

law enforcement

different

in writing

possible measures, such as the use of data) and related to data management

limited to data security measures.

The Authority found that Customer 2 in the operator's room in his own building

determines the purpose of the data processing carried out, the data processing (including the device used)

makes and executes certain relevant decisions (when, with regard to what

monitoring of live images, what he might be watching). Client 2 with professional advice,

contributed to the definition of data management tools with suggestions, that is

in making certain decisions regarding the circumstances of data management.

Based on all of this, Customer 1 and Customer 2 are considered joint data controllers.

Cooperation Agreement between Client 1 and Client 2 sent to the Authority

it does not contain any specifics or substantive rules with the camera system

in relation to related data management. Customer 2 also made a contradictory statement

about its role, since the camera system considers it to be common data management – otherwise correctly

activities carried out during its use, and at the same time Customer 1 as the sole data controller
considers it during the procedures in which it records a camera recording.
Because it is a law, an international treaty or a binding legal act of the European Union
it is not determined by the fulfillment of obligations related to joint data management
division of their responsibilities, so Infotv. 25/B. Pursuant to paragraph (1) of §
For Customer 1 and Customer 2 as joint data controllers
was created and
it is necessary to enter into a public agreement.
At this point, the Authority points out the unlawful deficiency that, despite the above, it is
Infotv. 25/B. Section (1) of the agreement, which settles the data controller
tasks and responsibilities related to the fulfillment of obligations - such as operation,
data security is affected
fulfillment, keeping records, and that
issues of handling incidents - did not arise between Customer 1 and Customer 2.
III.2.2 Concerning the keeping of the electronic diary and data security measures
violation of provisions
The Authority established that it was established at the headquarters of Client 2 and Client 1
with the conditions provided for the physical protection of operator rooms and server rooms, a
City Guard camera room,
found elements
(workstation and server) lacks the conditions of physical security, since it is directly one
a door opening from a public area merely means the physical security of the premises.
The Authority found that Infotv is infringing. 25/F. § (1) point d) and together
the requirement of accountability and data security is also that the public
supervisors (and in the period before the date of the on-site inspection by Client 2
persons performing activities) enter the system with the same login; not individually

it is recorded who entered and performed data management operations in the system. The

the range of persons performing data management activities based solely on their job title

can be narrowed down to the range of admissions.

The Authority points out that Infotv. 25/I. § (3) in points c) and e).

enforcement of data security measures, as well as Infotv. 25/F. included in §

in order to comply with the electronic log provisions, if

different data controllers or different ones employed by each data controller

users related to data management

depending on it is different

are entitled to carry out data management activities, then the different rights correspond to them

or the data controller

performance of their tasks

system there

rights

20

camera system

to modernize,

further development,

access authorization setting is required. Set for each user

relating to various data management operations

and up-to-date on rights

records must be kept. Neither Customer 1 nor Customer 2 was aware of such records

To make available to the authority.

The Authority established that Infotv. 25/F. the obligation contained in paragraph (4) of §

according to which in the data controller and data processor register, as well as the electronic one

data recorded in a diary must be kept for ten years after the deletion of the processed data, no

can be fulfilled, since the activities of the users - according to the statements of Customer 1 and Customer 3 -

It can be viewed for 30 days. E unlawful practice - Article 4(4) of the Crime Directive

in violation of the principle of accountability laid down in paragraph - the data management Authority

resulted in the impossibility of its control by the

regarding that customers

his activities are not documented, and so neither are the contents of his statements

can be checked in accordance with the law.

The Authority draws attention to the fact that, in this regard, Infotv. According to § 75, paragraph (6).

the exemption rule cannot be applied, given that it was examined in the present procedure

automated data management system was not created before May 6, 2016. THE

public domain

uniform

for the development of a video management system 16.06.2020. business contract concluded on

based on According to the statements of Customer 1 and Customer 3, he graduated in this system

user activity logging is 30 days according to the factory setting, but this can be changed

also for a longer interval.

The Authority found that 3 employees of Customer violated Infotv. 25/D. § (3)

point a) of paragraph - according to which, during the activity of the data processor, only

acts on the basis of the written instructions of the data controller - with the knowledge and instructions of the data controllers

without modification, deletion and creation of roles was carried out by Client Authority 1

completion of his on-site inspection at the headquarters and completed at the headquarters of Customer 2

in the period between the start of your on-site inspection.

III.2.3. Sanctions

Infotv. Other measures based on subsection (1) bg) and subsection (4) of § 61

may also impose a fine ranging from one hundred thousand to twenty million forints.

With regard to Customer 1 and Customer 2, in view of the above, the Authority has approved Infotv. Section 61 (1)

according to subparagraph b) of paragraph b) it is established within the framework of the surveillance system

method of data management

in view of the common data controllers

to the absence of an agreement regulating the distribution of their responsibilities related to data management,

and for breaching data security and accountability requirements.

The Authority examined the necessity of imposing the fine. Customer 3 above violates the law

in relation to its activities, the Authority does not consider it proportionate and sufficient merely to

establishing the fact of illegality, taking into account the act and the 3 persons of the Customer

mitigating and aggravating circumstances. The Authority is the whole of the case

considering its circumstances, in order to protect personal data in the future, decided to

that it is necessary to impose a fine in relation to Customer 3. The amount of the fine

determined in his statutory discretion. Infotv. Section 61 (4)

according to paragraph 1, the amount of the fine that can be imposed can range from one hundred thousand to twenty million

forints.

When determining the amount of the data protection fine, the Authority as a mitigating circumstance

took into account that

illegality

21

- the modification, deletion and creation of new roles by Customer 3 employees

carried out without instructions, on his own authority,

- The Authority has not previously established personal data against Customer 3

violation of the law related to its management;

- the nature and severity of the violation is of minor importance.

When determining the data protection fine, the Authority took it as an aggravating circumstance

considering that

- the act took place immediately before the Authority's on-site inspection,

at a time when Customer 3 was already aware of the purpose of the Authority's proceedings,

already made a partial statement about the conditions of data management and knew what would happen

the next location of the inspection, where the Authority will determine the conditions of data management

to investigate;

- Customer 3 violated his legal obligation, according to which in the course of his activities

acts solely on the basis of the written instructions of the data controller.

Based on the above, the Authority, according to the relevant part, the maximum amount that can be imposed is one

the amount of a data protection fine corresponding to a fortieth of the total of the cases

based on its circumstances, as proportionate and deterrent in relation to Customer 3.

The Authority is Infotv. Based on points a) and b) of § 61, paragraph (2), the decision is made by the Customer

also ordered the disclosure of his identification data, as it is a violation of law

affects a wide range of persons and is a body performing a public task

with his activity

brought in context.

ARC. Other questions

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

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

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

facilitating its free flow within.

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

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

a decision can be appealed through an administrative lawsuit.

* * *

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

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

the administrative lawsuit against falls within the jurisdiction of the court, the lawsuit is governed by Section 13.(3) of the Civil

Code

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

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

(1) is applicable - the court based on point b) of § 27.§ (1) of the Criminal Code

Legal representation is mandatory in a lawsuit within its jurisdiction. According to subsection (6) of § 39 of the Civil Code – if

the law does not provide otherwise - the filing of the claim is administrative

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

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

of 2015 on the general rules of electronic administration and trust services

CCXXII. Act (hereinafter: E-Administration Act) according to Section 9 (1) point b).

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

22

The place and time of submitting the statement of claim is determined by § 39. (1) of the Code of Civil Procedure. THE

information on the possibility of a request to hold a hearing can be found in Kp.77.§ (1) and (2)

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

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

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

exempts the party initiating the procedure.

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

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

client in the Authority's final decision

did enough, that is

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

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

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

Pursuant to § 134, enforcement - if it is a law, government decree or municipal regulation

in official matters, the decree of the local government does not provide otherwise - the state

undertaken by the tax authority.

Budapest, February 14, 2022.

Dr. Attila Péterfalvi

c. professor

not as an obligation

president

23