Case number: NAIH / 2020/643/6.

(NAIH / 2019/5963.)

Subject: Infringement decision

The National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority) shall be the

[…] lawyer.

(office address: […]) represented by the trade union […] represented by three natural persons

hereinafter together referred to as the "Applicants"), represented by […], an individual lawyer,

Operating in the dining room of his requested factory building or in another work room

on 6 September 2019 concerning the management of data related to the electronic monitoring system

the following decisions in the data protection authority proceedings initiated.

I. The Authority

IN ITS DECISION

1) Dismisses the applications of the Applicants.

Ex officio

2) states that the Applicant is bound for the purpose in the work room called teqball

the principles of data management and necessity, data saving and fair data management

inconsistently, the personal data of the employees were handled by the camera in the absence of a proper legal basis

monitoring and unlawful processing

did not provide adequate prior information. By doing so, Claimant violated the natural

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

repealing Directive (EU) 2016/679 on the free movement of persons and repealing Directive 95/46 / EC

Article 5 (1) (a) to (b) and Article 6 of the General Data Protection Regulation

and Article 13 (1) to (2).

3) finds that in the absence of a proper legal basis in the dining room, the Applicant,

the camera handled the personal data of the employees in violation of the principle of data protection

monitoring and unlawful processing

did not provide adequate prior information. By doing so, Claimant violated the general

Article 5 (1) (c) and Article 13 (1) to (2) of the Data Protection Regulation.

4) The Authority shall examine the Applicant ex officio

500,000, ie five hundred thousand forints

data protection fine

obliges to pay.

***

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

centralized revenue collection target settlement forint account (10032000-01040425-00000000

Centralized direct debit IBAN: HU83 1003 2000 0104 0425 0000 0000)

to pay. When transferring the amount, NAIH / 2020/643. JUDGE. number should be referred to.

If the Applicant fails to meet the obligation to pay the fine within the time limit, the above

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

interest,

2

which corresponds to the central bank base rate in force on the first day of the calendar half-year affected by the delay

me.

In the event of non-compliance with the fine and the late payment allowance or the prescribed obligations, the Authority shall:

initiate the implementation of the decision.

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

within 30 days of the application to the Metropolitan Court in an administrative lawsuit

can be challenged. The emergency does not affect the time limit for bringing an action. The application is lodged with the

It shall be submitted to the Authority, by electronic means, which shall forward it together with the case file to the

court. The request to hold a hearing must be indicated in the application. The whole personal

For those who do not receive an exemption, the fee for the administrative lawsuit is HUF 30,000, the lawsuit is material

subject to the right to record duties. Legal representation is mandatory in proceedings before the Metropolitan Court.

EXPLANATORY STATEMENT

I. Facts, antecedents

I. 1. Applicants shall represent the […] trade union representing them and the legal person representing that trade union

in their application to the Authority on 5 September 2019

complained that in May 2019 the Applicant had installed an electronic monitoring system in the

in the dining room used by the workers in the factory building of the

a room designated for meals or breaks. In addition, according to the request

separate from the cameras, a work primarily used by two workers

A camera was also installed in the room, which, based on its angle of adjustment, was used exclusively by the workers

used to monitor. According to the application, there is more different information about whether it is viable

or who can see the saved recordings, and the range of such persons may be so wide that - a

According to the applicants, this raises serious data protection concerns. According to the request, a

the installation of a camera surveillance system was not properly notified in advance to

stakeholders. After installing the system, verbally as much information was given to the person on site

workers that now operate a camera system in those premises, however, neither

the purpose and legal basis of the use or the place and time of storage of the recording

information, either orally or in writing, despite repeated requests for it, even in writing.

In their application, the Applicants requested the Authority to conduct proceedings to establish the infringement

and to take a decision to remedy the injurious situation in which the

Authority to order the Applicant to dismantle the cameras.

The Authority notified the Applicant of the initiation of the official data protection procedure and the facts

invited him to make a statement or provide information in order to clarify

I. 2. On the basis of the statements of the Applicants and the Applicant and the documentary evidence attached by them

it can be stated that the cameras were installed by a representative of […], who is the manager of the Requested Company

had the right to admin, but according to their statements, one of them recorded the recordings

neither viewed nor saved, they were not used for any other purpose. Not with data processing

no one was entrusted and no one other than them had access to the system.

According to the Applicant's statement, both premises are primarily for property protection purposes

two cameras were installed. In the dining room only for the benefit of the workers and his

they were installed at their request as a series of thefts occurred. By 5 employees of the Applicant

he confirmed in a signed statement that the employees acknowledge that they have requested the camera.

The so-called teqball room has two assembly tables and above these tables

placed two cameras, which are the primary asset for the protection of manufacturing technology

and recorded and verified the workflow. In addition, specifically for the desktop

surveillance cameras were needed because of compliance with the manufacturing process, possible

deficiencies and complaints can only be checked afterwards, and they have been protected by the same cameras

would also have employees in the circle of behaving properly. According to the statements

however, not only two permanent staff may work in this room, but also the number of staff and

the personality of the employees is constantly changing, it also depends on the given job.

In connection with the legal basis of data processing, the Applicant stated that as an employer a

Act V of 2013 on the Civil Code (a

hereinafter referred to as the Civil Code), according to which responsibility shall be assumed for the

also in mitigation. In addition, aspects relating to work and occupational safety

needs to be considered. Furthermore, the employees involved in the employment contract or its

(including the so - called Privacy Statement) have agreed to the

data management (Law of 2011 on the right to information self-determination and freedom of information)

CXII. Act (hereinafter: Infotv.) § 3 point 5 and Infotv. Section 5 (1) (b) and (c)

Based on). In addition, the Applicant's data management information for its employees

according to which the legal basis for data processing is the protection of vital interests. Additional statement of the Applicant

However, the legal basis for data processing is essentially Article 6 of the General Data Protection Regulation.

All the pleas in law under Article 1 (1) existed, with the exception of the plea in law under point (e).

According to point 8 of the statement of the Applicant dated 30 October 2019, neither pictorial nor audio was not recorded. However, according to paragraph 2 of this statement, teqball room camera was designed to adhere to the production technology, the workflow to pick up. According to the Applicant's statement dated 10 February 2020, teqball is also camera was needed in the room because the production process was followed, any objections, deficiencies and complaints can only be checked afterwards. That is, based on these statements it can be concluded that the cameras took pictures. This is supported by the Applicant also point 33 of the data management information for employees, which is the personal data processed mentions an image of the employee in the data set.

The Applicant's statement further provided orally, in writing, and with boards and multiple education workers were informed that cameras were in operation, but none at all they are not used in any way, they do not record. In addition, all employees involved attended the participation in the training and the completion of the training by signing them. The Requested It also states that there are separate regulations for the camera system and the employees also acknowledged this by signing their employment contract.

In addition, the Applicant is requested to initiate official data protection proceedings took steps to dismantle the cameras at the same time as it became aware of them. To prove everything a The applicant sent signed declarations, minutes and documents to the Authority.

However, it should be noted that the Applicant disputed the Applicants during the proceedings representative […] trade union, as in his opinion he does not work trade union, has no collective agreement and no separate agreement trade union and therefore cannot represent the Applicant's employees. The Requested in addition, since the […] trade union was not operating with the Applicant trade union, so it is not entitled to act by proxy.

II. Applicable legal provisions

Pursuant to Article 2 (1) of the General Data Protection Regulation, the General Data Protection Regulation
shall apply to the processing of personal data in a partially or fully automated manner,
and the non - automated processing of personal data which:
are part of a registration system or are part of a registration system
they want to do.
Infotv. Pursuant to Section 2 (2), the general data protection decree is the one indicated therein
shall apply with the additions provided for in
Infotv. Pursuant to Section 38 (2), the Authority is responsible for the protection of personal data, and
the exercise of the right of access to data in the public interest and in the public interest
free movement of personal data within the European Union
promoting.
Infotv. Pursuant to Section 38 (2a) of the General Data Protection Decree, the supervisory authority
the entities under the jurisdiction of Hungary
as defined in the General Data Protection Regulation and this Act
Authority exercises.
Infotv. Pursuant to Section 38 (3) (b), within the scope of its responsibilities under Section 38 (2) and (2a)
as defined in this Act, in particular at the request of the data subject and ex officio data protection
official procedure.
Infotv. Pursuant to Section 60 (1), the enforcement of the right to the protection of personal data
the Authority shall, at the request of the data subject, initiate a data protection authority procedure.
Unless otherwise provided in the General Data Protection Regulation, data protection was initiated upon request
CL of the General Administrative Procedure Act 2016. Act (a
hereinafter: Ákr.) shall apply with the exceptions specified in the Information Act.
According to Article 4 (11) of the General Data Protection Regulation: "consent of the data subject" means the data subject
voluntary, specific and well-informed and unambiguous declaration of will,
by which the statement concerned or the act of confirmation is unequivocally expressed,

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

Under Article 5 (1) (a), (b), (c) and (f) of the General Data Protection Regulation:

personal data:

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

("legality, fairness and transparency");

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

in a way incompatible with those objectives; not in accordance with Article 89 (1)

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

and further processing for historical research or statistical purposes ("purpose limitation").

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

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

[…]

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

ensure the adequate security of personal data, the data is unauthorized

5

or unlawful handling, accidental loss, destruction, or damage

protection against privacy ("integrity and confidentiality"). "

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

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

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

purposes

treatment;

(b) processing is necessary for the performance of a contract to which one of the parties is a party; or

to take steps at the request of the data subject before concluding the contract

required;

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

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

necessary for its protection;

(e) the exercise of a public interest or the exercise of official authority vested in the controller

necessary for the performance of its task;

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

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

or fundamental rights and freedoms which call for the protection of personal data,

especially if the child concerned. "

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

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

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

each of them:

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

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

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

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

legitimate interests of a party;

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

(f) where applicable, the fact that the controller is a third country or international organization

personal data and the Commission's decision on adequacy

existence or absence thereof, or in Article 46, Article 47 or the second subparagraph of Article 49 (1)

in the case of the transfer referred to in the first subparagraph, an indication of the appropriate and suitable guarantees,

and the means by which copies may be obtained or made available

reference.

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

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

provide the data subject with the following additional information:

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

aspects of its definition;

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

access, rectification, erasure or restriction of their processing and may object to such

against the processing of personal data and the right of the data subject to data portability;

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

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

does not affect the lawfulness of the processing carried out on the basis of the consent prior to the withdrawal;

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

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

based on or a precondition for concluding a contract and whether the person concerned is obliged to be personal

data and the possible consequences of providing the data

failure;

6

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

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

understandable information on the significance of such processing and on the data subject

its expected consequences. "

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

acting in its corrective capacity:

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

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

(b) condemn the controller or the processor if he or she has breached his or her data processing activities

the provisions of this Regulation;

(c) instruct the controller or processor to comply with the conditions laid down in this Regulation

request for the exercise of his rights;

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

in a specified manner and within a specified period, in accordance with the provisions of this Regulation;

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

(f) temporarily or permanently restrict the processing, including the prohibition of the processing;

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

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

shall notify the addressees with whom it is addressed in accordance with paragraph 1 and Article 19

or with whom personal data have been communicated;

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

revoke a certificate issued by the. or instruct the certification body not to issue the

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

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

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

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

suspension. "

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

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

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

in the Member State of the offense, if the person concerned considers that his or her personal

processing of data in breach of this Regulation.

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

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

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

whether it is necessary to impose an administrative fine or the amount of the administrative fine

In each case, due account shall be taken of the following:

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

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

the extent of the damage suffered;

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

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

any measures taken to

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

and the technical and organizational measures taken pursuant to Article 32;

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

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

the degree of cooperation to alleviate

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

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

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

in detail;

(i) if previously against the controller or processor concerned, on the same subject matter

- has ordered one of the measures referred to in Article 58 (2), the person in question

compliance with measures;

(j) whether the controller or processor has kept itself approved in accordance with Article 40

codes of conduct or approved certification mechanisms in accordance with Article 42;

and

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

financial gain or avoidance as a direct or indirect consequence of the infringement

loss.

[…]

5. Infringements of the following provisions in accordance with paragraph 2 shall not exceed 20 000 000

With an administrative fine of EUR 1 million or, in the case of undertakings, the previous financial year in full

up to 4% of its annual worldwide turnover,

the higher amount shall be charged:

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

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

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

transmission in accordance with Articles 44 to 49. in accordance with Article

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

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

or a request to permanently restrict or suspend the flow of data

failure to provide access in breach of Article 58 (1).

[…] ”

Furthermore, under Article 88 (1) and (2) of the General Data Protection Regulation:

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

rules may be laid down to ensure the protection of rights and freedoms

with regard to the processing of employees' personal data in connection with employment,

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

or collectively agreed obligations, work management,

planning and organization, equality and diversity in the workplace, the workplace

health and safety, the protection of the employer 's or consumer' s property, and

the individual or collective exercise and enjoyment of employment-related rights and benefits

for the purpose of termination of employment.

2. These rules shall include appropriate and specific measures which are appropriate

to protect the human dignity, legitimate interests and fundamental rights of the data subject, in particular

transparency of data management within a group of companies or a joint economic activity

intra-group transfers and on-the-job checks

systems.

[…] ”

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

shall exercise the powers set out in paragraph 1, taking into account the principle of proportionality, in particular:

by the law on the processing of personal data or by the European Union

in the event of a first breach of the requirements laid down in a mandatory act of the

in accordance with Article 58 of the General Data Protection Regulation

take action by alerting the controller or processor. "

8

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

according to: “An employee’s right to privacy may be restricted if the restriction is an employment relationship

absolutely necessary for reasons directly related to its purpose and proportionate to the achievement of the objective. THE

the manner, conditions and expected duration of the restriction of the right to privacy, and

the circumstances justifying the necessity and proportionality of the employee in writing in advance

shall be informed. "

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

can be checked. In this context, the employer may also use technical means, a

inform the employee in writing in advance. "

III. Decision

III. 1. General remarks

According to the definitions of the General Data Protection Regulation, a person's face is an image

view personal data, view live images through the camera, take pictures,

as well as any operations performed on personal data, such as viewing images

considered as data management.

Location of non-recording equipment and direct observation of the transmitted image

similar to the person conducting the surveillance (e.g., police officer, security guard, workplace manager, etc.)
on-site presence, although to some extent. Today, with the help of technology (e.g.
because it is possible to observe much more widely than it is personal
presence, so observation of the transmitted images in these cases for more detailed control
allows. Furthermore, the transmission or observation of live images is usually for some purpose
can be considered as part of a unified data management process, of which
as a result, the data controller makes some decision based on viewing the live image. Therefore
technical observation as a substitute for personal presence, i.e., cognition of images in general
does not constitute data processing under the provisions of the Data Protection Regulation unless
if the technique used during the observation does not offer the possibility to observe
additional information on the natural person concerned.
An additional condition for this is that the cameras are not really a secret surveillance tool, but
serve as a substitute for the presence of the person entitled to inspect, so that it is clearly visible in all cases
they must be placed in such a way as to be brought to the attention of those concerned by other means.
It follows that, although information contrary to the Authority is available to it
as to whether or not the cameras in question are recording, data management
realized.
In the present case, the Authority
operating cameras and related data processing. However, all this a
Authority examined ex officio and generally for employees, not the Applicants
on the basis of his request, given that the Applicants' legal representative did not know beyond a reasonable doubt
certify to the Authority that the Requested is related to electronic surveillance
his data processing did indeed extend to the Applicants as data subjects. Lack of stakeholder quality
the Authority rejected the Applicants' request and the right to the protection of personal data
examined the alleged infringements of its own motion in order to

III. 2. The purpose of the data processing and its suitability for this purpose

On the basis of the declarations and the documents available to the Authority, the Applicant shall all

both cameras in the dining room and in the teqball room were installed primarily for security purposes,

and, in addition, the cameras installed in the teqball room comply with the production technology, and

workflow was recorded and verified, roughly checking the work performance of employees.

In connection with the camera surveillance used at the workplace, the starting point is Mt., which

Pursuant to Section 42 (2) (a), on the basis of the employment contract, the employee is obliged to a

to perform work under the direction of the employer. In accordance with this, the legislator has amended Section 52 (1) of the

Mt.

Paragraph 1 (b) and (c) defined as a fundamental obligation of the employee that a

an employee is required to be available to his employer during his working hours and to perform his work in general

with the required expertise and diligence, the rules, regulations,

carried out according to instructions and customs. In order to maintain these legal obligations, the legislator is

Mt. 11 / A. § (1) provides for the possibility for the employer to employ the employee a

check your employment-related behavior, even if it is a technical device

also by applying. This right may involve the processing of personal data.

Section 9 (2) of the Mt. further states that the employee has the right to privacy at that time

may be restricted if the restriction is for a reason directly related to the purpose of the employment relationship

absolutely necessary and proportionate to the achievement of the objective. On how to restrict the right to privacy,

conditions and expected duration, and the necessity and proportionality of the

the employee must be informed of the circumstances in writing in advance.

In connection with the cameras operated by the Applicant and challenged by the Applicants

recognizes the designated purpose of data protection as a legitimate purpose of data protection, however, teqball

In the case of cameras installed in a room, the purpose of the protection of property cannot be interpreted, as the Authority

based on snapshots of the areas monitored by the cameras

in his opinion, there is no property to be protected in the room.

Adherence to production technology and recording and verification of work processes as further

with regard to the purpose of data processing, the Authority is of the opinion that they cannot be interpreted as they are not

it is clear why workflows need to be recorded and what and who needs them

prove. Given that the purpose of this data processing as defined by the Applicant is not

it is clear, in the Authority's view, that the data processing does not comply with the purposeful data processing

principle.

If the processing had a legitimate purpose, Article 5 (1) of the General Data Protection Regulation

It follows from the principle of data protection under paragraph 1 (c) that the lawfulness must be examined

whether the purpose of data processing can be achieved in a reasonable or proportionate manner by other means, and

whether a

the suitability and relevance of personal data for the purpose of their processing.

The need for data processing in this premises would be considered justified by the Authority if

if specifically for reasons such as making production technology more efficient

necessary, i.e. to do this periodically it is necessary to work with cameras

and then to analyze the recordings, which is, for example, new as a result of the analysis process

manufacturing technology will be introduced. However, according to the Applicant's statements, these cameras

was not served for this purpose, so the need for data management could not be justified either.

Consequently, the Authority concludes of its own motion that the data processing did not comply

purpose-based data management, nor the principle of necessity, in violation of the general data protection

the principle of purposeful data processing under Article 5 (1) (b) of

the principle of data protection under Article 5 (1) (c) of the Data Protection Regulation.

10

Based on the information available to the Authority, the cameras operated by the Applicant a

they could also be used to control workers. Mt. 11 / A. § (1) of the employer

check the employee in the context of the employment relationship, even by technical means,

however, in writing in advance - Article 13 (1) to (2) of the General Data Protection Regulation

shall also inform the employee, avoiding that the

cameras become a secret surveillance tool.

Cameras for employees and the activities they perform are permanent, with no explicit purpose

cannot be operated to monitor. Electronic is considered illegal

the use of a monitoring system to monitor the behavior of workers at work

influence. It is not possible to operate cameras that are aimless or not

for a clearly defined purpose, exclusively to the workers and the work performed by them

activity is observed. Exceptions are workplaces where workers

his life and physical integrity may be in imminent danger, so an exceptionally operable camera, for example

in assembly halls, smelters, industrial plants or other sources containing hazards

facilities. It should be emphasized, however, that - from the case law of the Constitutional Court

as follows - only then can a camera be operated on the workers' life and physical

in order to protect the integrity of the

danger cannot be a constitutionally acceptable purpose for data processing. However, all this to the employer

must prove in the balancing test. In the case of surveillance for property protection purposes, also a

the employer must prove that there are in fact circumstances which

justify the placement of each camera and otherwise the intended purpose cannot be achieved.

In the case of surveillance for the purpose of property protection, another important requirement is that it is special for the

employer

it must be borne in mind that the angle of view of a given camera is essentially that of the property to be protected

and should not become the work of workers as a result of the above

as a tool for monitoring

For cameras operated in the dining room, electronic should be considered

the general principle of the applicability of surveillance systems is that it cannot be

to place the camera in rooms where the operation of the camera would violate human dignity,

consequently the principle of fair data management. There can be no cameras along this principle

be placed in particular in changing rooms, showers and toilets, taking into account that

observation in these premises is a particular violation of the right to human dignity. In addition, the

The Authority also considers that an electronic monitoring system cannot be used as such

nor in a room designated for the purpose of taking a break between employees as

for example, a dining room for employees. An exception to this may be the case where

if there is any property to be protected in this room (such as a food and drink vending machine),

in connection with which an employer interest can be demonstrated (for example, employees

the equipment was damaged several times and the damage had to be borne by the employer). In this case

a camera can be placed in the room for this specific purpose, but it is special for the employer

you must therefore pay attention to the angle of view of the camera - taking that into account

necessity and proportionality - may be limited to the property to be protected.

However, given that it was sent to the Authority from the area monitored by the cameras

based on the snapshots taken, the angle of view of the two cameras was not focused on a property to be protected,

but for the whole room, the Authority ex officio finds that the Applicant with these cameras

Article 5 of the General Data Protection Regulation

The principle of data retention referred to in paragraph 1 (c).

11

III. 3. Legal basis for data processing

The Authority examined of its own motion the electronic monitoring carried out by the Applicant

the legal basis for data processing.

Article 6 (1) of the General Data Protection Regulation on the legal basis for data processing

the legal basis referred to in point (e) relied on in relation to each of the pleas in law referred to in paragraph 1

with the exception of the Civil Code. and employment contracts with employees.

The grounds on which the processing of personal data may be lawful may be general

Article 6 (1) of the Data Protection Regulation. Although the general privacy

Article 88 of the Regulation is national in relation to employment-related data processing

within the framework set out in the provision

these national legislative measures comply with Article 6 (1) of the General Data Protection Regulation.

may not extend the grounds set out in paragraph 1. As a result, the data controller is

the legal bases set out in Article 6 (1) (a) to (f) of the General Data Protection Regulation

may base the lawfulness of its data processing on one of these, these lawfulness conditions

in the absence of compliance, the processing of data is merely a provision of national law

is not sufficient to substantiate its legality, even if it is general

The Data Protection Regulation explicitly requires a

national legislative action.1 The controller shall base his data processing on any legal basis (s),

you must be able to prove its existence. However, it is not lawful to rely on each of the pleas in law,

relying on it as one of the legal bases.

1. It follows that the Civil Code itself. rules do not generally qualify as

the rule governing the lawfulness of data processing.

2. As a legal basis for consent under Article 6 (1) (a) of the General Data Protection Regulation

it may be duly invoked if the conditions are met. The contribution shall be

be based on adequate information as defined in the General Data Protection Regulation,

must be voluntary and the will of the data subject to consent must be specifically,

by a clear statement or unequivocal statement

to declare.

The consent must therefore be based on adequate information. The Authority shall take this decision

III. Section 7 analyzes in detail the information on the data processing of the Requested, here only

indicates that they did not comply with Article 13 of the General Data Protection Regulation

requirements.

The contribution must also be voluntary. Regarding voluntary contribution, however

in accordance with Article 29 of the Data Protection Directive2 prior to the General Data Protection Regulation

established the Data Protection Working Party3 (hereinafter referred to as the "Data Protection Working Party")

also stated in its resolution that the employee-employer relationship is questionable

the possibility of voluntary consent can in principle only be invoked when

1

See, for example, Article 6 (3) of the General Data Protection Regulation.

95/46 / EC on the protection of individuals with regard to the processing of personal data and on the free movement of such

data

Directive of the European Parliament and of the Council

2

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

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

Privacy Board has stepped in.

3

it is clear that the employee receives unconditional “benefits” from data processing and not

he may suffer any disadvantage in the event of a refusal to process data. The world of work is concerned

therefore, as in the present case, another legal basis based on the legitimate interest of the employer

the use of data management is justified.

Therefore, there was no legal basis for consent in the case of the present data processing

applicable.

3. With an employment contract as Article 6 (1) (b) of the General Data Protection Regulation

In the context of the legal basis under Article

data management related to camera surveillance, as is also the Privacy Policy

Working Group 6/2014. lawful under Article 7 of Directive 95/46 / EC

opinion on the concept of the interests of the data protection4 - in which the general data protection regulation was written

interpretation of the contractual legal basis

- in the present case, an employment contract - that this plea cannot be interpreted broadly. THE

The contractual legal basis does not apply to situations where the processing is not in fact the
necessary for the performance of the contract, but is unilaterally imposed on the data subject by the controller. THE
data management related to camera surveillance is not in itself necessary in all cases a
performance of an employment contract and is not the result of an agreement (especially if
internal regulations and other non-statutory employment relationships at the given workplace
therefore not covered by this data processing at issue in the present case
may be the legal basis of the employment contract.
4. Legal obligation under Article 6 (1) (c) of the General Data Protection Regulation
its legal basis is also inapplicable in the present case, since it can be said in the context of that plea that
that the fulfillment of a legal obligation on the controller to process the data
provided for in Union law or in the law of a Member State
must have a legal basis. However, the General Data Protection Regulation does not require that
each specific data processing operation should be subject to separate legislation. It may also be sufficient to
if a single legal act serves as a legal basis for several data processing operations which are
based on a legal obligation to the controller. The purpose of the data processing is also EU or Member State
shall be determined by law. The General Data Protection Regulation on the processing of personal data
The general conditions for the legality of
the precise rules for the designation of the data controller, the personal data subject
the type of data, the data subjects, the organizations to which the personal data may be communicated,
restrictions on the purpose of data processing, the duration of data storage and other,
necessary measures to ensure lawful and fair data processing
may be determined by Infotv. In accordance with Section 5 (3).
Legislation may also impose a legal obligation to handle personal data
the law does not specify the circumstances of the data processing. If so
The legislation prescribing mandatory data management does not fully comply with Infotv. Section 5 (3)
and does not contain the circumstances of the data processing, the data controller shall apply

communicate the principles under the general rules governing the processing of personal data; and

guarantees which the legislator failed to provide.

There may also be cases where the legislation contains only a general authorization

to carry out a specific activity involving the processing of personal data. An example of such a case is

A 6/2014. Reviews can be found at the following link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

4

13

The provision of the Mt. according to which the employee's conduct related to the employment relationship

can be checked. The law then provides for the possibility (and not the obligation) of control,

nor does it prescribe data processing as an obligation, therefore the legal basis of data processing is also different (a

legitimate interest of the employer).

5. Pursuant to the legal basis under Article 6 (1) (d) of the General Data Protection Regulation

data processing that is vital for the data subject or another natural person is also lawful

necessary to protect its interests. Vital interests of another natural person

personal data may be processed with reference to the processing in question

cannot be done on any other legal basis. However, given that in the present case the data processing

its legal basis may be a legitimate interest and is therefore not applicable.

6. Under Article 6 (1) (f) of the General Data Protection Regulation, it may then be lawful

data processing if the data processing is in the legitimate interest of the data controller (or a third party)

necessary and not preceded by any personal data from the data subjects

interest or fundamental right and freedom requiring data protection. So the data controller then

act with due diligence when initiating data processing based on a legitimate interest

prior to, for example, the Data Protection Working Party will carry out the 6/2014. in its opinion no

balance of interests described in which it identifies its own (or third party’s) legitimate

as a counterparty to the weighting, in cases such as the present

the interests of the employee, the fundamental right concerned, and shall only start or continue processing

if, on the basis of the weighting of the two interests, it is established that the interest of the data subject does not precede his

own

meg.5 In this balance of interests, it is always based on the specific facts of the case - and not abstract

should also take into account the reasonable expectations of those concerned.

It follows from all this, as well as from recital 39 of the General Data Protection Regulation

the data management must be specified by the employer in advance prior to the data processing

should have a purpose for camera surveillance. For this purpose (which is also

in most cases) actual and real, a

adapted to the activity of the employer, the market situation and the job of the employees

they must be.

It can therefore be concluded that the legal basis for the present data processing is general

legitimate interest under Article 6 (1) (f) of the Data Protection Regulation

and, after due consideration of the interests involved, in the present case

notwithstanding the legitimate purpose of the processing

it is proved that the given data management would have been necessary or proportionate.

7. The Authority therefore concludes that the data processing referred to by the Applicant

of the pleas in law, only the legal basis for a legitimate interest could have been applied in the dining room

however, due to the need for data management

and its proportionality was not justified and the Authority established the principle of data saving

therefore, as there was no justification for this applicable legal basis, the Applicant

also infringed Article 6 of the General Data Protection Regulation.

5

A 6/2014. Article 7 (f): legitimate interests Point 3 (page 25)

III. 4. Fair data management

The Authority shall act in accordance with Annex III to this Decision. Paragraph 2 found that by the Applicant, the teqball the data processing carried out in the room did not comply with the principle of purposeful data management, necessity and violated the principle of data protection. Sent to the Authority by the cameras However, on the basis of snapshots of the areas observed, the Authority considers that cameras were capable of aimless, continuous surveillance of workers. In view of this, the The Authority examined of its own motion the extent to which the data processing complied with fair data processing requirement. The integrity of data management is closely linked to the protection of human dignity In relation to unfair data processing practices, the data subjects are not only personal data protection, but also its right to human dignity. Therefore respect for human dignity is an absolute limit to camera surveillance, therefore cameras cannot be operated by workers and the activity they perform is permanent to observe. Electronic is also considered illegal and unfair the use of a monitoring system that does not have a clear, clearly defined purpose, but merely observes the work in general. The Constitutional Court ruled in 36/2005. number stated in its decision that “electronic surveillance is therefore suitable for penetrate the private sphere, capture intimate (sensitive) life situations even in such a way that the the person concerned does not even know about the admission or is not in a position to consider such the admissibility of the recordings and their consequences. The observation thus made a beyond the right to privacy - in a broader and deeper sense - to human dignity may generally affect the right to The essential conceptual element of the private sector is precisely that it is concerned against his will, others should not be able to penetrate or look into it. If you don't want to insight takes place, then not only is the right to privacy in itself, but it is other elements of entitlement within the scope of human dignity, such as freedom of self-determination or the right to bodily integrity may be violated. " In the present case, by contrast, Annex III to the present decision Not according to point 2 cameras operated for a clear purpose in the teqball hall - Annex III to this Decision. According to point 5

without adequate prior information - which were suitable for the workers' express purpose

all-day observation. This observation is contradicted by the above

principle of fair data management, the Authority therefore concludes of its own motion that the

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

principle of data management.

III. 5. The requirement for adequate prior information and the principle of transparency

An essential requirement for data processing related to camera surveillance at work,

that they are concerned about data management in advance is appropriate, transparent and easy to understand

receive information. The Authority therefore examined of its own motion the extent to which the Applicant had done so

fulfill this obligation.

Both the Mt. and the General Data Protection Ordinance require that data subjects be informed

on the conditions relating to data processing. Mt. 11 / A. § (1)

general information obligation regarding the processing of personal data by the general

must also be complied with in accordance with the provisions of the Data Protection Regulation, ie in general

data protection regulation, setting out the circumstances in which e

the employer must inform the employees in this regard. The data controller shall be provided with the information

in a concise, transparent, comprehensible and easily accessible form, in a clear and comprehensible manner

in writing or otherwise, including, where appropriate, by electronic means

way too. However, the Authority will in any case recommend the written format on the grounds that -

also the principle of accountability under Article 5 (2) of the General Data Protection Regulation

consequently - the data controller, the employer must prove and certify the appropriate prior

information has been provided.

According to the Applicant's statement, orally, in writing, as well as with boards or in the context of several trainings

they indicated to workers that cameras were operating, the live image they were transmitting

however, they are not used in any way, they do not make recordings. At the same time,

as set out in Annex III to this Decision. Although it contains information contrary to the Authority
whether or not the cameras in question are recording,
data management was implemented, so the Applicant had to comply with the information
obligation. In addition, according to the Applicant's statement, all interested parties were aware of the
cameras that have been trained, attended, and completed the training
certified by their signatures. According to the Applicant's statement, there are also separate regulations for the
camera system and the employees take note of this by signing their employment contract
were taken.
However, on the basis of the documents sent to the Authority, it can be concluded that the Applicant is separate
does not have a policy on the camera system. Made for employees only
Section 33 of the Data Management Information mentions the personal data processed about the employee
(taken by the security service in the event of a security incident, about the employee
imaging), the purpose of data management (security incidents - fire, accident, technological failure,
loss of property, etc. Discovery of the cause), legal basis (protection of vital interests), duration (a
time of investigation of security incident, employer action based on security incident
the limitation period for bringing an action against the measure), the recipient of the data (the
staff involved in the investigation of an incident: the position held by the employee
the head of the department or another employee appointed by him, exercising the authority of the employer or by him
other assigned employee, office manager, employee performing work safety duties).
However, this information is not specifically the camera complained of by the Applicants
surveillance-related data processing, although the Applicant also e
marked the data management information sent as a basis for informing employees
on data management. With regard to this prospectus, it can be stated that it does not comply with the general
requirements of the Data Protection Regulation, as it does not provide information for individual cameras
and their purpose, the area, the subject, the
or whether the employer monitors the camera directly or recorded.

Furthermore, the prospectus does not provide information on the specific duration of storage of recordings

the rules for reviewing the recordings and the purpose for which they are recorded

can be used by the employer.

It should also be noted that the prospectus contains 38 data management purposes and the above data management

circumstances (scope of data processed, purpose of data processing, legal basis, duration, data

addressee) for each of them, while at the beginning of the prospectus, all

on the rights and enforcement of data subjects

information that does not, however, cover the specific circumstances of the camera surveillance, e.g.

exclusion of the right to rectification - and does not include the general data protection in a transparent manner

special circumstances relating to the execution of requests from data subjects pursuant to Article 12 of this Regulation

(for example, extending the deadline for completing the request). Nor does the

information pursuant to Article 15 (3) of the General Data Protection Regulation

nor the right to copy it.

With regard to any oral information, the Authority further notes that its

its content has not been proven.

16

On the basis of the above, the Authority concludes of its own motion that the Applicant has not provided

adequate information on the data management and related information to the Applicants and

other employees concerned, in breach of Article 13 of the General Data Protection Regulation.

Furthermore, recital (60) of the General Data Protection Regulation

The principle of transparency and fair treatment referred to above requires that the

the data subject of the fact and purpose of the processing and any such

information necessary to ensure fair and transparent data management, which

the Applicant did not comply with this requirement, violated Article 5 of the General Data Protection Regulation.

article. The principle of transparency referred to in paragraph 1 (a).

III. 6. Rejection of the request to dismantle the cameras

The Authority shall reject the relevant part of the application and shall not hold it of its own motion

necessary to order the Applicant to dismantle the cameras, as the Applicant is

The Data Protection Authority, after becoming aware of the initiation of the proceedings, provided the

The decommissioning of the cameras complained of by the applicants, that is to say, it terminated the unlawful data

processing.

III. 7. Procedural rights of the trade union representing the Applicants

With respect to the requested procedure, the Applicant disputed during the proceedings representing the Applicants

[…] Trade union representation rights. At the request of the Authority, the legal representative of the Applicants shall:

[…] To the trade union by sending a power of attorney from the three Applicants

right of representation, ie in the opinion of the Authority, the right of representation

based on power of attorney, not union quality.

Anyone may make a report or complaint regarding a general inquiry into data processing, and

It is up to the Authority to decide whether to conduct an ex officio procedure and, if so,

which type of procedure.

III. 8. Sanctioning

The Authority examined of its own motion whether a data protection fine against the Applicant was justified.

imposition. In this context, the Authority shall comply with Article 83 (2) of the General Data Protection Regulation and

Infotv. 75 / A. § considered all the circumstances of the case and found that the present

In the case of infringements detected during the procedure, the warning shall be neither proportionate nor dissuasive

sanction, it is therefore necessary to impose a fine.

The specific deterrent effect of the Authority in imposing fines is to encourage the Applicant to

to carry out its data management activities and activities consciously and not the data subjects

as an object, but as a genuine right holder, securing their resulting rights, personal

information and other conditions necessary to exercise control over the processing of their data.

In general, it is necessary to make it clear to all data controllers in a similar situation

to make the processing of personal data requires increased awareness cannot be common sense in this area

to act without negligence, without taking any proactive measures

trusting that there will be no detriment to personal information is effectively uncontrolled

treatment. Such negligent conduct disregards the rights of the data subject and, as such,

it cannot go unpunished.

17

In setting the amount of the fine, the Authority took into account, in particular, that:

Infringements by the applicant under Article 83 (5) (a) of the General Data Protection Regulation

and (b) constitute an infringement in the higher category of fines.

The Authority took into account as an aggravating circumstance that:

-

the Applicant deliberately, in a hierarchical relationship, with his position as an employer

committed an infringement in breach of Article 83 (2) (b) of the General Data Protection Regulation

point];

-

the Applicant installed the cameras without complying with Article 25 of the General Data Protection Regulation.

and 32 have taken the necessary technical and organizational measures and

would have taken into account additional data protection requirements [general data protection

Article 83 (2) (d) of the Regulation].

The Authority took into account as an attenuating circumstance that

-

to convict the Applicant for violating the General Data Protection Regulation

has not taken place [Article 83 (2) (e) of the General Data Protection Regulation];

-

the Applicant's knowledge of the commencement of the data protection authority proceedings

dismantled the cameras complained of by the Applicants [General Data Protection Regulation

Article 83 (2) (c) and (f)]

-

the Authority has exceeded the administrative deadline [Article 83 (2) of the General Data Protection Regulation

paragraph (k)].

The Authority did not consider the general data protection to be relevant when setting the fine

circumstances within the meaning of Article 83 (2) (g), (h), (i) and (j) of

cannot be interpreted in this context.

In view of the above, the Authority will set the level of the fine close to the minimum

amount. The Authority took strong account of mitigating circumstances,

whereas, in its view, this could also be the case for the Applicant

general and special prevention purposes due to a data breach.

The turnover of the Applicant in 2019 was more than HUF 1,000 million, so the imposed data protection

the fine shall not exceed the maximum fine that may be imposed.

ARC. Other issues:

The powers of the Authority shall be exercised in accordance with Infotv. Section 38 (2) and (2a) determine the jurisdiction of

the country

covers the whole territory.

The present decision of the Authority is based on Art. 80-81. § and Infotv. It is based on Section 61 (1). The decision is

Ákr. Pursuant to Section 82 (1), it becomes final upon its communication. The Ákr. Section 112 and Section 116 (1)

and § 114 (1) is the subject of an administrative lawsuit against the decision

place of redress.

***

The Ákr. Pursuant to Section 135 (1) (a), the Applicant is entitled to the statutory interest rate

is obliged to pay a late payment allowance if it fails to meet its payment obligation on time.

The Civil Code. 6:48. § (1), in the case of a debt owed, the debtor is in arrears

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

shall pay default interest at the same rate as the basic interest.

The rules of administrative litigation are laid down in Act I of 2017 on the Procedure of Administrative Litigation (a

hereinafter: Kp.). A Kp. Pursuant to Section 12 (1) by decision of the Authority

The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (3) a)

Pursuant to point (aa) of the Act, the Metropolitan Court has exclusive jurisdiction. A Kp. Section 27 (1)

(b), legal representation is mandatory in litigation falling within the jurisdiction of the Tribunal. A Kp. § 39

(6) of the application for the entry into force of the administrative act

has no suspensive effect.

A Kp. Section 29 (1) and with regard to this, Act CXXX of 2016 on Civil Procedure. law

Applicable according to § 604, electronic administration and trust services are general

CCXXII of 2015 on the rules of According to Section 9 (1) (b) of the Act, the customer is legal

representative is required to communicate electronically.

The time and place of the submission of the application is Section 39 (1). The trial

Information on the possibility of requesting the maintenance of the It is based on § 77 (1) - (2). THE

the amount of the fee for an administrative lawsuit in accordance with Act XCIII of 1990 on Fees. Act (hereinafter:

Itv.) 45 / A. § (1). From the advance payment of the fee, the Itv. Section 59 (1)

and Section 62 (1) (h) shall release the party initiating the proceedings.

If the Applicant does not duly demonstrate the fulfillment of the required obligation, the Authority shall

considers that it has failed to fulfill its obligations within the prescribed period. The Ákr. According to § 132, if the Applicant

has not complied with an obligation contained in the final decision of the authority, it shall be enforceable. The Authority

decision of the Ákr. Pursuant to Section 82 (1), it becomes final with the communication. The Ákr. Section 133

enforcement, unless otherwise provided by law or government decree

ordering authority. The Ákr. Section 134 of the Enforcement - if law, government decree

or in the case of a municipal authority, a decree of a local government does not provide otherwise

carried out by a state tax authority. Infotv. Pursuant to Section 61 (7) in the decision of the Authority

to perform a specific act, conduct or tolerate a specific act

the Authority shall enforce the decision in respect of the standstill obligation

implements.

Budapest, July 17, 2020

Dr. Attila Péterfalvi

President

c. professor