 File No.: PS/00178/2022

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and based on

to the following

BACKGROUND

FIRST: The General Police Directorate, Moncloa-Aravaca Police Station (in

successive National Police), dated 11/16/2020 filed a claim with the

Spanish Data Protection Agency against the entity MUXERS CONCEPT,

S.L., with NIF B87345369 (hereinafter, the claimed party or MUXERS). The motives

on which the claim is based are as follows:

The National Police gives an account of the complaint made before the Police Group

Judicial by five workers of a restaurant belonging to the claimed party,

for the “finding of an audio recording system in the company locker room”,

hidden in a false ceiling; as well as the proceedings instituted for that reason.

Provides a copy of the complaints outlined, in which the complainants declare having

found in the employee toilet, where their lockers are also located, a

alleged video surveillance camera and sound recorder, plugged in and on

conditions of use (three of the five complaints refer only to a

microphone). They also state that they were not informed about the installation of

These devices.

The National Police also provides a copy of a record, dated 10/27/2020, extended to

proceed to the intervention of a "Microphone with number Air Space AA003", and

photographs showing the location of this device in a false ceiling. According to

It is stated in this Act that the interested person who witnesses the intervention of the Police

Nacional states “that the seized microphone is owned by the company Muxers

Concept, S.L., CIF…”.

On the other hand, on 04/20/2021, a claim was received from A.A.A.

(hereinafter, the complaining party), also directed against the entity MUXERS, in the

stating that on 10/27/2020, in the company of other colleagues,

discovered at his workplace (the same one referred to in the claim of the

National Police) “the placement of audio/video recording cameras in the toilets

corresponding to the changing rooms of the workers”.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, of Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), the claim received from the National Police was transferred

to the claimed party, so that it could proceed with its analysis and inform this Agency in

within a month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

(hereinafter, LPACAP) by electronic notification, was not collected by

the person in charge, within the period of making available, understanding rejected

in accordance with the provisions of art. 43.2 of the LPACAP on 12/20/2020, as stated

in the certificate that works in the file.

Although the notification was validly made by electronic means, assuming

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, by way of

informative, a copy was sent by mail that was reliably notified in

date 01/18/2021. In said notification, he was reminded of his obligation to relate

electronically with the Administration, and they were informed of the means of access to

said notifications, reiterating that, in the future, it would be notified exclusively

by electronic means.

On 02/17/2021, this Agency received a response letter provided by the

Respondent, stating the following:

The system, which was installed by the entity Teknometric Biometric Solutions and New

Technologies, S.L. (Teknometric) on 06/20/2018, it has 22 cameras inside

of the premises, 2 exterior cameras on the facade, 1 recording equipment and 4 microphones of

preamplified audio, without any device in the locker room or in the

toilets.

On the existence of a contract by which a third party is commissioned to view and/or

listening to the images and/or audios, informs that there is a contract with the company

“Stop Alarma since the installation corresponds to the video surveillance system”. I know

attached contract and certificate of connection to alarm center and video certificate

check with that company.

In relation to the purpose of the installation of video surveillance equipment, it indicates that

Said purpose is “the access control of people, merchandise… security of the

goods and people”. In this regard, it notes that a written communication was made to

the workers since the opening and the letters signed in agreement by

each worker about the placement, its nature and its location.

Regarding the causes that gave rise to the claim, the respondent adds that the

rarefaction of the labor relationship caused by the reduction of working hours of the

workers and not having collected the amounts owed by the partial ERTE, motivated

that the workers raised the false ceiling and dragged the micro from the office (where if

there is a microphone) and they will take him to the locker room area, not to the bathrooms, and from there all the controversy.

Additionally, all the workers have criminally denounced the owner of the company, and there have been dismissals with the corresponding lawsuits in the Court of the Social.

There are complaints by the company against the aforementioned workers for this

incident, which led to the dismissal of some of them, among others the manager who relinquishing his duties, he admitted the entry of people from outside the premises and he hatched a whole plan in order to ask for money by all means, as it has been.

Attached are the complaints from the company, the letters reducing the working day, which explain the real reasons for this matter, which has nothing to do with the placement of cameras or microphones since the company has never placed them and appears on the location map from the first day of opening of the premises and the communication to female workers since August 2018.

Therefore, according to the respondent, it is difficult for the workers to say, as say they were unaware of the location of the security systems when they were knowledgeable from the beginning of its existence, purpose, location, etc.

For more details, the lawyer of one of the complainants has asked the company 35,000 euros for this compensation issue for not going to trial.

Everything along the lines that we have said of pressuring the company to compensate the workers or to reinstate them.

With your response, provide the following relevant documentation:

. Location map of the cameras and microphones (22 interior cameras, 2

exterior cameras, 1 recording equipment, 4 audio microphones

preamps). According to this plan, prepared by Teknometric, the microphones

they are installed at the entrance to the restaurant, in the room where they are located

the tables and bar of the establishment (more than XX tables of different dimensions

-between and six stalls- and 12 bar stalls), in an office and in a room of

small size whose use is not specified in the plan.

. Camera location photos

. Provide a photograph in which the existence of an informative poster can be seen

of the existence of the cameras, located inside the premises.

. Provides an invoice from the installer of the Teknometric cameras, detailing

the installed system, made up of 22 interior cameras, 2 exterior cameras, a recorder

video surveillance and 4 audio outputs with hard disk, and "4 hidden microphones

preamplified"; and technical report issued by this same entity on the

installation of these devices on 06/20/2018. This report indicates

that MUXERS was informed "of the regulations and legality regarding the notice of

their employees before the placement of audio microphones".

. "Video verification certificate" and "Certificate of connection to alarm center"

issued by the entity Stop Alarmas, S.L.U. The latter includes a section

called "Verification" in which the "Sequential" options are marked,

Image" and "Bidirectional". The "Audio" option is not checked.

. 10 documents dated 08/20/2018, with the label "Communication to the

worker of the existence of video surveillance cameras whose images can

be used to control labor obligations and duties". to information

contained in these documents is excerpted in the Fourth Proven Fact.

. Complaint filed with the National Police by the administrator of the entity

MUXERS, for damage caused to the staff locker room on the date

10/27/2020 ("the roof is broken and the microphone cables that were in the

inside hanging"). This document contains the manifestations of the

complainant. Among them, the following:

"That the complainant states that they are microphones, that in the employment contract comes

specified the audio and video recording, and that they themselves have signed".

"That at 1:20 p.m. another indicative of the National Police comes to

seize the microphone from the locker room, all of which is reflected in a Record of

Intervention of Effects of which they deliver a copy to the complainant".

THIRD: On 02/22/2021, in accordance with article 65 of the LOPDGDD,

The claim filed by the National Police was admitted for processing.

Similarly, the claim made by the claimant was admitted for processing in

date 05/07/2021.

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

question, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

. A request for information was sent to the claimed party, by postal mail

Addressed to the same address where the notification of the outlined transfer was made

in the previous Antecedent, without in this case the notification could be practiced

(it was returned with the indication "unknown").

. The National Police, on 12/03/2021, informed the Inspection Services that

the police report of the Moncloa-Aravaca Police Station, has led to the opening

Preliminary Proceedings No. ***PROCEEDINGS.1, followed up in the Court of Instruction No.

XX of Madrid.

. Requested information from the aforementioned Court of Instruction on the possible

responsibility of the claimed party in the installation of the devices of

audio and video recording in the changing rooms and toilets used by the workers of the

establishment to which the claims refer, no reply was received from

said court during the period of these investigative actions.

Thus, it was agreed to declare the expiration of the aforementioned prior actions of

research and open new research actions, as well as incorporate the

same the documentation that integrates the expired actions.

The response from the Investigating Court was received on 01/26/2022, stating

reports that what has been done to date (01/18/2022) in the Procedure

Abbreviated that follows under the number ***DILIGENCIAS.1, "the

responsibility of the entity MUXERS CONCEPT, S.L.”.

FIFTH: On 05/13/2022, by the General Subdirectorate for Data Inspection

You can access the information related to the MUXERS entity in “Axesor” (“Informe

monitor”). (...).

SIXTH: On 05/20/2022, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the MUXERS entity, in accordance with the

provided in articles 63 and 64 of the LPACAP, for the alleged violation of article

6 of the RGPD, typified in article 83.5.a) of the aforementioned Regulation; and rated as

very serious for prescription purposes in article 72.1.b) of the LOPDGDD.

In the opening agreement it was determined that the sanction that could correspond,

attended the existing evidence at the time of opening and without prejudice to what

resulting from the instruction, would amount to a total of 20,000 euros (twenty thousand euros).

The notification of this opening agreement to the claimed party, in which

granted a term to formulate allegations and propose evidence, it was sent by means of the

Electronic Notification Service, although it was not collected by the

claimed within the period of availability.

Although the notification was validly made by electronic means, assuming

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, with

date 06/09/2022 a new notification attempt was made by post, being

returned the shipment due to an incorrect address, even though it was addressed to the

registered office of the entity that appears in the Mercantile Registry.

Likewise, on 06/23/02022, a document was published in the Official State Gazette

announcement of notification of the opening of proceedings. In said announcement, it is informed

the party complained against about the possibility of obtaining a copy of the opening agreement.

SEVENTH: Notification of the aforementioned start-up agreement in accordance with the established rules

in the LPACAP and after the term granted for the formulation of allegations,

has verified that no allegation has been received by the respondent party.

Article 64.2.f) of the LPACAP - provision of which the respondent was informed

in the agreement to open the procedure - establishes that if no

allegations within the stipulated period on the content of the initiation agreement, when

it contains a precise statement about the imputed responsibility,

may be considered a resolution proposal. In the present case, the agreement

beginning of the sanctioning file determined the facts in which the

imputation, the infraction of the RGPD attributed to the claimed and the sanction that could

prevail. Therefore, taking into consideration that the respondent has not

formulated allegations to the agreement to initiate the file and in attention to what

established in article 64.2.f) of the LPACAP, the aforementioned initial agreement is

considered in this case proposed resolution.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

1. the MUXERS entity is responsible for the video surveillance system installed in the

premises in which it carries out its activity on 06/20/2018. It's about a

establishment open to the public dedicated to restoration.

2. The video surveillance system outlined in the First Proven Fact, in addition to

video surveillance cameras, has four audio microphones

preamplified, installed at the entrance to the restaurant, in the room where they are

located the tables and bar of the establishment (more than 30 tables of different

dimensions -between and six seats- and 12 bar seats), in an office and in a

small room whose use is not specified.

This system has a video surveillance recorder and 4 audio outputs with

HDD.

3. The intended purpose of installing this equipment is access control

of people and goods, the safety of goods and people, as well as the

control of labor obligations and duties.

4. At the time of the installation of the video surveillance system, the entity MUXERS

provided its workers with an informative document with the label "Communication to the

worker of the existence of video surveillance cameras whose images can be

used to control labor obligations and duties". According to these documents,

the party claimed informs the worker who signs it as follows:

"In accordance with Law 5/1999… INFORMS… (name and surname of the worker) of the

recording through video cameras in the internal and external facilities of the company of

which is a treatment responsibility of Muxers Concept, SL in which they remain

stored your personal data, including your image and sound obtained, recorded and

captured through cameras and video cameras, for the following purposes:

I. Surveillance

Internal and external surveillance of the company's facilities..., in order to provide

compliance with the security operation and to prevent risks that affect the security and

protection of people, premises and patrimonial assets as well as to denounce, when

necessary, made before the competent authorities or meet requirements of the

themselves.

II. Quality and work performance

Control of the quality and labor performance of the workers as well as verification of the

fulfillment by… (name and surname of the worker) of their obligations and duties

labor.

III. disciplinary sanctions

The images and sound captured by the video surveillance cameras may be used to

the detection by Muxers… of criminal acts or labor offenses included in the agreement

collective… as evidence when sanctioning

…the technical instruments used…respect the right to privacy, within the

legitimate exercise of the power of business surveillance.

5. Due to complaints made by restaurant workers, the

The National Police appeared at the MUXERS establishment and drew up a record dated

10/27/2020, extended to proceed with the intervention of a “Microphone with

Air Space numbering AA003”. This document includes some photographs in which

the location of this device is seen in a false ceiling. As stated in these Minutes,

the interested person who, on behalf of MUXERS, witnesses the intervention

of the National Police states “that the seized microphone is property of the

company Muxers Concept, S.L., CIF…”.

In its response to the claim transfer process, MUXERS stated that the

microphone intervened by the National Police was in the office set up in the

establishment.

FOUNDATIONS OF LAW

Yo

In accordance with the powers that article 58.2 of the RGPD grants to each authority of

control and as established in articles 47, 48.1, 64.2 and 68.1 of the Organic Law

3/2018, of December 5, on the Protection of Personal Data and guarantee of the

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures

processed by the Spanish Agency for Data Protection will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures.

Image and voice are personal data

II

The physical image and voice of a person, in accordance with article 4.1 of the RGPD, are a

personal data and its protection, therefore, is the subject of said Regulation. In the article

4.2 of the RGPD defines the concept of "treatment" of personal data.

Images and voice captured by a camera or video camera system are data

of a personal nature, so its treatment is subject to the regulations of

Data Protection.

It is, therefore, pertinent to analyze whether the processing of personal data (image and voice

of the workers in the establishment to which the claims refer, whose

ownership corresponds to the claimed party, and of the natural persons who attend

as customers to said establishment, open to the public) carried out through the

denounced video surveillance system is in accordance with the provisions of the RGPD.

III

Infringement

Article 6.1 of the RGPD establishes the assumptions that allow the legalization of the

treatment of personal data.

The permanent installation of a video camera system for reasons of

Security has a legitimate basis in the LOPDGDD, whose explanatory statement indicates:

“Together with these assumptions are included others, such as video surveillance… in which the legality of the

treatment comes from the existence of a public interest, in the terms established in the

article 6.1.e) of Regulation (EU) 2016/679”.

Regarding the treatment for video surveillance purposes, article 22 of the LOPDGDD

establishes that natural or legal persons, public or private, may carry out

carry out the processing of images through camera systems or video cameras

in order to preserve the safety of people and property, as well as their

installations.

This same article 22, in its section 8, provides that "The treatment by the

employer of data obtained through camera systems or video cameras

subject to the provisions of article 89 of this organic law.

On the legitimacy for the implementation of video surveillance systems in the field

employment, Royal Legislative Decree 1/1995 of 03/24 is taken into account, approving

the revised text of the Workers' Statute Law (LET), whose article 20.3

points out:

"3. The employer may adopt the measures it deems most appropriate for surveillance and control

to verify the fulfillment by the worker of his labor obligations and duties,

keeping in its adoption and application the consideration due to its dignity and taking into account

account, where appropriate, the real capacity of workers with disabilities.

The surveillance and control measures admitted include the installation of

security cameras, although these systems must always respond at the beginning

of proportionality, that is, the use of video cameras must be proportional to the purpose

pursued, this is to guarantee the security and fulfillment of the obligations and

job duties.

Article 89 of the LOPDPGDD, specifically referring to the "right to privacy

against the use of video surveillance and sound recording devices in the place

of work" and the treatment of personal data obtained with camera systems or

video cameras for the exercise of control functions of workers, allows

that employers can treat the images obtained through systems of

cameras or video cameras for the exercise of control functions of the

workers or public employees provided, respectively, in article 20.3

of the Workers' Statute and in the public function legislation, provided that

These functions are exercised within their legal framework and with the limits inherent to the

same.

In relation to the recording of sounds, the aforementioned article 89 of the LOPDGDD

sets the following:

"two. In no case will the installation of sound recording systems or

video surveillance in places intended for rest or recreation of workers or

public employees, such as changing rooms, toilets, dining rooms and the like.

3. The use of systems similar to those referred to in the previous sections for the

recording of sounds in the workplace will be allowed only when they are relevant

risks to the safety of facilities, assets and people arising from the activity

that is developed in the workplace and always respecting the principle of proportionality,

the minimum intervention and the guarantees provided for in the previous sections. suppression

of the sounds preserved by these recording systems will be made according to what

provided in section 3 of article 22 of this law."

On the other hand, it is interesting to note that, according to the doctrine of the Constitutional Court, the

Recording of conversations between workers or between them and customers is not justified

for the verification of the fulfillment by the worker of his obligations or duties.

In Judgment dated 04/10/2000 (2000/98), issued in rec. no. 4015/1996, it

declares the following:

"In this sense, it must be taken into account that the managerial power of the employer,

essential for the smooth running of the productive organization and expressly recognized

in art. 20 LET, attributes to the employer, among other powers, that of adopting the measures that

considers more opportune of vigilance and control to verify the fulfillment of the worker of

their labor obligations (art. 20.3 LET). But this faculty must occur in any case,

as is logical, within due respect for the dignity of the worker, as we expressly

The labor regulations remember it (arts. 4.2.e and 20.3 LET)…

… it should be remembered that the jurisprudence of this Court has repeatedly insisted on the

full effectiveness of the fundamental rights of the worker within the framework of the relationship

employment, since this cannot imply in any way the deprivation of such rights for

those who provide service in productive organizations... Consequently, and as

this Court has also affirmed, the exercise of such rights only admits

limitations or sacrifices to the extent that it operates within an organization

that reflects other constitutionally recognized rights in arts. 38 and 33 EC and that

imposes, according to the assumptions, the necessary adaptability for the exercise of all of them...

For this reason, the premise from which the appealed Judgment starts, consisting of

affirm that the workplace does not constitute by definition a space in which the

right to privacy on the part of the workers, in such a way that the conversations that

keep workers among themselves and with customers in the performance of their work activity

are not covered by art. 18.1 EC and there is no reason why the company cannot

know the content of those, since the aforementioned right is exercised in the field of

worker's private sphere, which in the workplace must be understood as limited to the

places of rest or recreation, changing rooms, toilets or the like, but not those

places where work is carried out...

…Such an affirmation is rejectable, since it cannot be ruled out that also in those

places of the company in which the work activity is carried out may occur

illegitimate interference by the employer in the right to privacy of the

workers, such as the recording of conversations between a worker and a

client, or between the workers themselves, in which issues unrelated to the relationship are addressed

work that are integrated into what we have called the sphere of development of the

individual (SSTC 231/1988, of December 2, FJ 4 and 197/1991, of October 17, FJ 3, by

all). In short, it will be necessary to attend not only to the place of the workplace where they are installed

by the company audiovisual control systems, but also to other elements of judgment (if

the installation is done or not indiscriminately and massively, if the systems are visible or have

been installed surreptitiously, the real purpose pursued with the installation of such

systems, if there are security reasons, due to the type of activity that takes place in the

work center in question, justifying the implementation of such means of control, etc.)

to elucidate in each specific case whether these means of surveillance and control respect the right to the privacy of workers. Certainly, the installation of such means in places of rest or recreation, changing rooms, toilets, dining rooms and the like is, a fortiori, harmful in any case of the right to privacy of workers, without further consideration, for obvious reasons... But this does not mean that this injury cannot occur in those places where the work activity is carried out, if any of the exposed circumstances that allows the business action to be qualified as an illegitimate intrusion into the right to privacy from the workers. It will therefore be necessary to attend to the concurrent circumstances in the event specifically to determine whether or not there is a violation of art. 18.1 EC.

…their limitation [of the fundamental rights of the worker] by the powers business can only derive good from the fact that the very nature of work contracted implies the restriction of the right (SSTC 99/1994, FJ 7, and 106/1996, FJ 4), either an accredited need or business interest, without its mere invocation being sufficient to sacrificing the fundamental right of the worker (SSTC 99/1994, FJ 7, 6/1995, FJ 3 and 136/1996, FJ 7)…

These limitations or modulations must be those that are indispensable and strictly necessary to satisfy a business interest worthy of guardianship and protection, in a that if there are other possibilities of satisfying said interest that are less aggressive and affect the right in question, it will be necessary to use the latter and not the more aggressive and affecting. It is, in short, the application of the principle of proportionality...

The question to be resolved is, therefore, whether the installation of microphones that allow the recording of conversations of workers and customers in certain areas... is adjusted in the event that concerns us to the essential requirements of respect for the right to privacy. To the In this regard, we must begin by pointing out that it is indisputable that the installation of capture and recording of sound in two specific areas... it is not without utility for the business organization, especially if one takes into account that these are two areas in which

significant economic transactions take place. Now, the mere utility

or convenience for the company does not simply legitimize the installation of hearing aids and

recording, given that the company already had other security systems than the

hearing system is intended to complement…

In summary, the implementation of the audition and recording system has not been in this case

in accordance with the principles of proportionality and minimum intervention that govern the modulation

of fundamental rights by the requirements of the interest of the organization

business, because the purpose pursued (to give a plus of security, especially before

possible claims from customers) is disproportionate to the sacrifice that

It implies the right to privacy of workers (and even customers...). This system

allows you to capture private comments, both from customers and workers...,

comments completely unrelated to business interest and therefore irrelevant from the

perspective of control of labor obligations, being able, however, to have

negative consequences for workers who, in any case, will feel constrained

to make any type of personal comment before the conviction that they are going to be

heard and recorded by the company. It is, in short, an illegitimate interference in the

right to privacy enshrined in art. 18.1 CE, since there is no definitive argument that

Authorize the company to listen to and record private conversations that workers…

keep with each other or with customers.

On the other hand, the processing of personal data is subject to the rest of the

principles of treatment contained in article 5 of the RGPD. We will highlight the

principle of data minimization contained in article 5.1.c) of the RGPD that

provides that personal data will be "adequate, relevant and limited to what is

necessary in relation to the purposes for which they are processed".

This means that in a specific treatment only the data can be processed.

timely personal, that come to the case and that are strictly necessary

to fulfill the purpose for which they are processed. The treatment must be adjusted and

proportional to the purpose to which it is directed. The relevance in the treatment of

data must occur both at the time of data collection and in the

subsequent treatment of the same.

In accordance with the above, the processing of excessive data must be restricted or

proceed to their removal.

The application of the principle of minimization of data to the case examined involves

that the installed camera or video camera system cannot obtain images or

sounds affecting the privacy of employees, resulting disproportionate

capture images or sounds in private spaces, such as changing rooms, lockers or

worker rest areas.

IV

Video surveillance obligations

In accordance with the foregoing, the processing of images through a system

of video surveillance, to be in accordance with current regulations, must comply with the

following requirements:

1.- Individuals or legal entities, public or private, can establish a system

video surveillance in order to preserve the safety of people and property,

as well as its facilities.

It must be assessed whether the intended purpose can be achieved in another less

intrusive to the rights and freedoms of citizens. personal data only

should be processed if the purpose of the processing could not reasonably be achieved by

other means, considering 39 of the RGPD.

2.- The images obtained cannot be used for a later purpose

incompatible with the one that motivated the installation of the video surveillance system.

3.- The duty to inform those affected provided for in articles

12 and 13 of the RGPD, and 22 of the LOPDGDD.

In this sense, article 22 of the LOPDGDD provides in relation to video surveillance

a system of “layered information”.

The first layer must refer, at least, to the existence of the treatment

(video surveillance), the identity of the person in charge, the possibility of exercising the rights

provided for in articles 15 to 22 of the RGPD and where to obtain more information about the

treatment of personal data.

This information will be contained in a device placed in a sufficiently

visible and must be supplied in advance.

Second layer information should be readily available in one place

accessible to the affected party, whether it is an information sheet at a reception, cashier, etc...,

placed in a visible public space or in a web address, and must refer to the

rest of the elements of article 13 of the RGPD.

4.- Images of public roads cannot be captured, since the treatment of

images in public places, unless there is government authorization, only

It can be carried out by the Security Forces and Bodies.

On some occasions, for the protection of private spaces, where

installed cameras on facades or inside, it may be necessary to ensure the

security purpose the recording of a portion of the public highway.

That is, cameras and video cameras installed for security purposes may not

obtain images of public roads unless it is essential for that purpose, or

it is impossible to avoid it due to their location. And in that case

extraordinary, the cameras will only be able to capture the minimum portion necessary to

preserve the safety of people and property, as well as its facilities.

Installed cameras cannot get images from third-party proprietary space

and/or public space without duly accredited justified cause, nor can they affect

the privacy of passers-by who move freely through the area.

It is not allowed, therefore, the placement of cameras towards the private property of

neighbors with the purpose of intimidating them or affecting their private sphere without cause

justified.

In no case will the use of surveillance practices beyond the environment be allowed.

object of the installation and in particular, not being able to affect public spaces

surrounding buildings, adjoining buildings and vehicles other than those accessing the space

guarded.

Images cannot be captured or recorded in spaces owned by third parties without the

consent of their owners, or, as the case may be, of the people who

find.

It is disproportionate to capture images in private spaces, such as

changing rooms, lockers or worker rest areas.

5.- The images may be kept for a maximum period of one month, except in

those cases in which they must be kept to prove the commission of acts

that threaten the integrity of people, goods or facilities.

In this second case, they must be made available to the authority
competent within a maximum period of 72 hours from the knowledge of the
existence of the recording.

6.- The person in charge must keep a record of treatment activities
carried out under its responsibility, including the information to which it makes
reference article 30.1 of the RGPD.

7.- The person in charge must carry out a risk analysis or, where appropriate, an evaluation
of impact on data protection, to detect those derived from the implementation
of the video surveillance system, assess them and, where appropriate, adopt the measures of
appropriate security.

8.- When a security breach occurs that affects the processing of
cameras for security purposes, whenever there is a risk to the rights and
freedoms of natural persons, you must notify the AEPD within a maximum period of
72 hours.

A security breach is understood as the accidental or accidental destruction, loss or alteration of
illicit of personal data transmitted, conserved or treated in another way, or the
unauthorized communication or access to said data.

9.- When the system is connected to an alarm center, it can only be
installed by a private security company that meets the requirements
contemplated in article 5 of Law 5/2014 on Private Security, of April 4.

The Spanish Agency for Data Protection offers through its website

[https://www.aepd.es] access to:

. the legislation on the protection of personal data, including the RGPD

and the LOPDGDD (section “Reports and resolutions” / “regulations”),

. the Guide on the use of video cameras for security and other purposes,

. the Guide for compliance with the duty to inform (both available in the

section “Guides and tools”).

It is also of interest, in the event of carrying out low-risk data processing, the

facilitates free tool (in the “Guides and tools” section), which, through

specific questions, allows to assess the situation of the person in charge with respect to the

treatment of personal data that it carries out, and where appropriate, generate various

documents, informative and contractual clauses, as well as an annex with measures

guidelines considered minimum.

v

administrative offense

The claim is based on the alleged illegality of the video surveillance system installed

by the claimed party in the premises where it develops its business activity, in

related to sound recording.

In this case, the fact that the claimed party is the owner and

responsible for the reported video surveillance system and, therefore, the person responsible for

the data processing involved in the use of said system. And neither does he

fact that the data processing carried out includes the collection and

storage of personal data relating to the voice of employees and customers.

It is also proven in the actions that said installation is carried out with

security and labor control purposes.

For this reason, on 08/20/2018, the respondent informed the workers

affected, including the complaining party, the installation of the

video surveillance, with capture and recording of images and sound, “for the purpose of

to comply with the security operation and to prevent risks that affect the

safety and protection of people, premises and property” and for the

“control of the quality and labor performance of the workers as well as verification

compliance… with their labor obligations and duties.”

The party complained against does not provide sufficient justification for these data treatments

(sound recording). The claimed party does not take into account the limits set forth in

article 20.3 of the Workers' Statute Law (LET); what is established in the

article 89.3 of the LOPDGDD, which admits the recording of sounds only when

risks are relevant and respecting the principles of proportionality and

minimal intervention; nor the doctrine of the Constitutional Court, already expressed, according to the

which the recording of conversations between workers or between workers and customers is not

justified by verification of compliance by the worker with his obligations or

homework.

The aforementioned article 89 of the LOPDGDD, beyond the prohibition of using these

video surveillance and sound recording systems in “places intended for

rest or recreation of workers or public employees, such as

changing rooms, toilets, dining rooms and the like”, expressly and in general,

establishes the submission of such systems to the legal framework and with the inherent limits

to the same, already mentioned above. This implies that it cannot be understood as

legitimate, without further condition, any system that does not include those spaces.

In this case, moreover, it is clear that one of the microphones was installed in the office used by workers. As has been proven, the system included the installation of four “hidden” microphones: at the entrance to the restaurant, in the dining room where the tables and bar of the establishment are located (more than 30 tables of different dimensions -between and six seats- and 12 bar seats), in an office and in a small room whose use is not specified in the plan. So, it turns out that some of these devices could violate the prohibition to install “sound recording systems… in places intended for rest or recreation of the workers..., such as changing rooms, toilets, dining rooms and analogues”, established in the aforementioned article 89 of the LOPDGDD.

On the other hand, the information provided to the workers refers to the "power of business surveillance". On this question, concerning the possibilities regarding the adoption of surveillance measures that attributes to the employer its power

direction, it is interesting to highlight some of the aspects declared in the Judgment of the Constitutional Court dated 04/10/2000, outlined in the Foundation of Law III:

“…this faculty must occur in any case, as is logical, within due respect for the dignity of the worker, as the labor regulations expressly remind us (arts. 4.2.e and 20.3 LET)…”.

“It must therefore be rejected… that the conversations that workers have with each other and with clients in the performance of their work activity are not covered by art.

18.1…”.

“…their limitation [of the fundamental rights of the worker] by the powers

business can only derive good from the fact that the very nature of work

contracted implies the restriction of the right (SSTC 99/1994, FJ 7, and 106/1996, FJ 4), either

an accredited need or business interest, without its mere invocation being sufficient to

sacrificing the fundamental right of the worker (SSTC 99/1994, FJ 7, 6/1995, FJ 3 and 136/1996,

FJ 7)…

These limitations or modulations must be those that are indispensable and strictly

necessary…”.

“…the mere utility or convenience for the company does not simply legitimize the installation of the

hearing and recording devices, given that the company already had other

security systems that the hearing system intends to complement…”.

Nor does it explain what the recording of conversations between the

workers, among themselves, between workers and customers, or between the latter among themselves,

in order to prove those circumstances, which does not provide the sole recording of

images.

Likewise, it is interesting to emphasize again that the recording of sounds includes the voice

of clients of the claimed party (two devices installed in the client area,

at the entrance to the restaurant and in the room where the tables and bar are located

establishment), which are unaware of the existence of the microphones.

Consequently, in this case, the capture of the voice is understood to be disproportionate.

of both workers and clients of the claimed party for the function of

intended video surveillance, to control compliance by workers with their

job duties and obligations. Note that voice recording involves

further invasion of privacy.

It is considered that the claimed party carried out data processing without having

legitimate basis, violating the provisions of article 6 of the RGPD, so they could

suppose the commission of an infringement typified in article 83.5 of the RGPD, which

provides the following:

“Infractions of the following provisions will be sanctioned, in accordance with section

2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company,

of an amount equivalent to a maximum of 4% of the total annual global turnover of the

previous financial year, opting for the highest amount:

a) the basic principles for the treatment, including the conditions for the consent to

tenor of articles 5, 6, 7 and 9;”.

For the purposes of the limitation period for infractions, the infraction indicated in the

previous paragraph is considered very serious in accordance with article 72.1.b) of the LOPDGDD,

which states that:

“Based on the provisions of article 83.5 of Regulation (EU) 2016/679, they are considered

very serious and will prescribe after three years the infractions that suppose a violation

substance of the articles mentioned therein and, in particular, the following:

b) The processing of personal data without the concurrence of any of the conditions of legality of the

treatment established in article 6 of Regulation (EU) 2016/679”.

SAW

Sanction

Article 58.2 of the RGPD establishes:

“Each supervisory authority shall have all of the following corrective powers

listed below:

(...)

d) order the person responsible or in charge of treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate,

in a certain way and within a specified period;

(...)

i) impose an administrative fine under article 83, in addition to or instead of

the measures mentioned in this section, according to the circumstances of each

particular case".

According to the provisions of article 83.2 of the RGPD, the measure provided for in article

58.2.d) of the aforementioned Regulation is compatible with the sanction consisting of a fine

administrative.

With regard to violations of article 6 of the RGPD, based on the facts

exposed, it is considered that the sanction that should be imposed is a fine

administrative.

The fine imposed must be, in each individual case, effective, proportionate

and dissuasive, in accordance with the provisions of article 83.1 of the RGPD.

In order to determine the administrative fine to be imposed, the

provisions of article 83.2 of the RGPD and article 76 of the LOPDGDD, regarding the

section k) of the aforementioned article 83.2 RGPD.

In this case, the following circumstances are considered aggravating:

. Article 83.2.a) of the RGPD: “a) the nature, seriousness and duration of the infringement,

taking into account the nature, scope or purpose of the processing operation

in question as well as the number of interested parties affected and the level of damage and

harm they have suffered."

. The duration of the infraction, considering that the installation of the devices

voice capture and recording took place in August 2018.

. The number of stakeholders: the alleged infringement affects all workers

and clients of the defendant.

On the other hand, it is estimated that there are mitigating circumstances

following:

. Article 76.2.b) of the LOPDGDD: “b) The link between the activity of the offender and the

personal data processing”.

The limited connection of the defendant with the performance of treatment of

personal data, considering the activity that it develops.

. Article 83.2.k) of the RGPD: “k) any other aggravating or mitigating factor applicable to

the circumstances of the case, such as financial gains or losses

avoided, directly or indirectly, through the infringement”.

The small business status of the Respondent and its volume of business.

(...).

Considering the exposed factors, the valuation reached by the fine for the

Violation of article 6 of the RGPD is 20,000 euros (twenty thousand euros).

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE MUXERS CONCEPT, S.L., with NIF B87345369, for a

infringement of Article 6 of the RGPD, typified in Article 83.5.a) of the RGPD, a

fine of 20,000 euros (twenty thousand euros).

SECOND: NOTIFY this resolution to MUXERS CONCEPT, S.L.

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following month or immediately after, and if

between the 16th and last day of each month, both inclusive, the payment term

It will be until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-050522

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es