 File No.: EXP202203617

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) on 03/18/2022 filed

claim before the Spanish Data Protection Agency. The claim is

directed against B.B.B. with NIF ***NIF.1 (hereinafter, the claimed party). The motives

on which the claim is based are the following:

The claimant states that until ***DATE.1 she was an employee of the

company of the claimed party, date on which he was notified of his dismissal

disciplinary action based on access to the content of voice recordings from the

video surveillance system that your work center has, extreme, the

audio recording by said system, of which the party was not informed

claimant, understanding that said circumstance is contrary to the regulations of

Data Protection.

It details that these recordings correspond to a conversation held with a

family on 03/02/2022, which took place inside the premises and outside working hours;

and another that he had with a client the next day, to whom he commented that one of the

machines prevented him from doing the jobs well. According to the complaining party, it is

two private conversations that were recorded by the video surveillance system,

as revealed by the party claimed in the messages sent by Whatsapp that

attached.

It adds that the information that was delivered to it on the aforementioned system of

video surveillance does not clarify whether or not the voice is recorded.

With your claim, provide the following documentation:

. WhatsApp conversation in which the claimed party alludes to the conversations

mentioned. This is a transcript of this alleged conversation collected

on a blank page with nothing to prove its authenticity.

. Image of a dismissal letter, dated ***DATE.1, stating

handwritten signature of the complaining party on the same date, as proof of its

delivery to the interested party. This letter communicates the termination of the employment relationship

for disciplinary dismissal, motivated by a "drop in work performance" and "bad

use of machinery", verified through the recordings of 03/02/2022. It does

reference, likewise, to the recording of a conversation in which the party

complainant "complains to a client about the state of the company's machinery,

blaming it for the errors in the orders".

. "Informative manual on the use of video surveillance systems" provided by the

claimed party to the claiming party, regarding the installed video surveillance system

in the workplace where the complaining party carried out its activity as

employee, in which the handwritten signature of the complaining party is recorded. Part of the

information contained in this document is outlined in the Proven Fact

Third.

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

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

forward LOPDGDD), said claim was transferred to the claimed party, for

to proceed with its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements established in the regulations of

Data Protection.

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

Public (hereinafter, LPACAP), was collected on 03/30/2022 as stated in the

acknowledgment of receipt in the file.

On 04/08/2022, this Agency received a written response in which the

Respondent party states the following:

". The person responsible for the treatment of the video surveillance system; B.B.B., with NIF… and

Contact email…

. The cameras installed in the premises of ***ADDRESS.1, have a security camera

video surveillance that is activated by stopping movement. This camera points to

a particular angle where the cash register is. It also has two

photodetectors located inside the premises. One of them above the camera

video surveillance with the same viewing angle as the video surveillance camera and the

second photodetector points to the rear of the premises. Both photodetectors only

activate when the alarm does and take three photos, these three photos

They can also be requested by the person in charge of the cameras to the person in charge of

treatment of the cameras, through the application.

Annex I: Photographs of these devices (camera and photodetectors) are attached together with

video surveillance posters, as well as photographs of the mobile screen used to

the vision of the images in the mobile application.

Photographs of the two posters in the premises that warn of the existence of

video surveillance area, these signs are located next to the cameras. in the same

It is appreciated expressly and clearly according to the RGPD and LOPDGDD, the

necessary information about who is responsible and the processing of your data,

what are the rights they can exercise and where to go to do so.

In the images of Annex I you can see the posters next to the cameras.

There are no monitors where captured images are shown and can be accessible

since these are only available in the mobile application provided by the

"Securitas Direct" treatment manager, to the mobile application is only authorized

your access the person responsible for the images, B.B.B..

Currently the company does not have workers on its account, therefore, there is no

authorized personnel in the establishment, nor are the cameras seen by the clientele,

given that they are only accessible by the mobile application that the person in charge of

treatment of the camera and the photodetectors puts at the disposal with a user and

password.

Documents are attached that prove that the worker A.A.A. with NIF ***NIF.2

who terminated his employment contract with the person in charge on ***DATE.1, knew the

existence of video surveillance cameras for labor control.

On ***DATE.2, the former worker was informed that a system had been installed

of video surveillance inside the premises and that this may be used to carry out a

Control of work performance of company workers. Said statement

is known and signed by it. In addition, you are given for more information a

Informative Manual on the use of video surveillance systems, also informed and

signed by the former and only worker.

The present document has as objective the knowledge of the installation and use of

video surveillance systems, derived from the need to carry out a control in the

accesses, as well as to the interior, in order to guarantee the security of the goods and

people.

The use of cameras or video cameras for security purposes implies the capture,

recording and storage of images that may contain character data

staff. Capture or recording may consist of an imaging system

associated or not with voice capture. This is how the staff is made aware through the

Information manual on the use of video surveillance systems.

Annex II: Information manual on the use of video surveillance systems and clause

informative, where the knowledge of these systems by the staff is accredited.

. The installation, maintenance and management of video surveillance and cameras have been

contracted and performed with the SECURITAS DIRECT Treatment Manager

SPAIN SAU…

Annex III: copy of the contract signed with the security company and technical report

of the video surveillance system.

. The video surveillance system records the images and keeps them for the period of

three days.

. Report on whether the video surveillance system installed in the establishment has

sound capture, as well as image.

The video surveillance system does have sound capture, in addition to capturing

of image. According to the Workers' Statute, the employer can establish the

surveillance and control measures that it deems most appropriate to verify the

fulfillment by the worker of his labor obligations and duties.

C / Jorge Juan, 6

28001 – Madrid

The video surveillance system takes into account the requirements of the LOPDGDD and the

GDPR; Principle of proportionality and the regulations on personal privacy.

Coinciding in their assessments of the business need to act in accordance with

the minimum intervention criteria, its maximum expression being the judgment of

proportionality, adequacy and balance.

The company established the measures it considered most appropriate for surveillance and

control to verify compliance by the worker with his obligations and

job duties.

Therefore, the same, taking as evidence the video surveillance cameras of the

and based on their right to take appropriate measures to control

labor;

On date ***DATE.1 communicates the termination of the employment relationship with A.A.A.,

through disciplinary dismissal given the reasons founded on a drop in

work performance where it is suspected and accredited through security cameras

video surveillance that the worker left tasks or orders unfulfilled.

In addition, it is demonstrated through the capture of the image a misuse of the

machinery, causing loss of material and time to the company.

As a result of poor work performance and in protection of business assets

it is decided to carry out a more exhaustive monitoring of the worker.

In the following days and given the previous suspicions, the audio is activated

of the camera, in which it is observed that the former worker misuses the

machinery... In the following days another fact is observed, the worker complains to

the clientele on the machinery of the company, blaming the errors on it and

causing discredit and possible economic losses to the company.

According to the events that occurred and the well-founded suspicions, the

resource used as a measure of control within the framework of the right to privacy

staff that would be limited to:

a) The suitability of the recording for the purpose intended by the company - verify

if the worker actually committed the suspected irregularities and if so

take appropriate disciplinary action.

b) The need for the measure -since the recording would serve as proof of such

irregularities.

c) The proportionality of control - temporarily, while demonstrating the

facts.

In short, this control function would be within the established legal limits.

in the art. 89.3 LOPDGDD, since it arises from a situation of suspicion

well-founded, that the means used is presented as the only viable one to carry out the

investigation necessary to guarantee a reliable result".

Ends the claimed part citing article 89.3 of the LOPDGDD.

Provide a copy of a document delivered to the claimant on ***DATE.2

(it has his handwritten signature and the indicated date, also handwritten), with the label

"Inform workers about the installation of cameras (Labor Control)". Part

of the information contained in this document is outlined in the Proven Fact

Third.

THIRD: On April 13, 2022, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

FOURTH: On May 9, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against the claimed party,

pursuant to the provisions of articles 63 and 64 of the LPACAP, for the alleged

infringement of article 6 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter GDPR), typified in article 83.5.a) of the aforementioned

Regulation; and classified 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,

attention to the existing evidence at the time of opening and without prejudice to the

that results from the instruction, would amount to a total of 6,000 euros.

Likewise, it was warned that the imputed infractions, if confirmed, may

entail the imposition of measures, according to the aforementioned article 58.2 d) of the GDPR.

FIFTH: Notified of the aforementioned start-up agreement in accordance with the rules established in

the LPACAP, the claimed party presented a pleading in which it requests the

procedure file based on the following considerations:

1. In response to what was stated by the complaining party regarding the ignorance of the

recording system, points out that in the conciliation document signed by the

admits the conversations held with the client and the knowledge about the

installation of the video and voice system.

In this regard, it clarifies that, in accordance with article 89 of the LOPDGDD, in no

case the audio and image recording was made in places intended for rest

or in places where private conversations would take place that could violate the

worker's right to privacy.

2. Understand that speaking ill of the company with a client can have consequences

negative, with economic repercussions and prestige in the company.

Therefore, in his opinion, two legally protected principles come into conflict: the

right of the worker protected by article 18.1 CE and the duties of good faith and loyalty

between the employer and the staff. Labor legislation protects that the worker

expose your complaints within the company, but another matter is to confuse the

freedom of opinion of the worker with the right to insult or use expressions

vexatious, insulting and to undermine the image of the company.

These conversations are recognized in the conciliation document signed by the

employee.

3. Nor was it necessary for complaints to be made directly to customers,

that harms the organization, influencing its success.

In this sense, the defendant considers that the power of direction of the

entrepreneur is essential for the smooth running of the organization, and

attributes the possibility of adopting surveillance and control measures such as recording,

This being proportional to the purpose and adjusted to the provisions of article 20.3 of the

Workers' Statute and article 89.3 of the LOPDGDD, which admits the

recording as an appropriate and proportionate measure in justified cases.

Regarding the tests, the following stands out:

. Voice recordings cannot be provided because they have been deleted after 30 days,

under applicable law. The defendant considers that this is essential in terms of this

proceedings.

. In contrast to what was expressed by the AEPD in the opening agreement, in relation to the "Informative manual on the use of video surveillance systems", which the authority of control does not consider conclusive in terms of information on voice pickup, should take into account what was expressed by the complaining party in the act of conciliation admitting that he was aware of the use of cameras with voice recording.

4. The question raised in this file has to do with the use of the recordings obtained by the video surveillance cameras of a company for the adoption of disciplinary dismissals, having informed the workers about the facility and its control purpose. You understand that said recording does not constitute a violation of data protection, since the worker knew the facility of the chamber, was in a conspicuous place, such circumstances being known by the hardworking, who knew the use that was going to be given to her.

The Judgment of the TC under number 39/2016, resolves a case in which a worker had been disciplinary dismissed. In this case they have not been used. cameras or video, since the claimed party has recognized the inappropriateness of dismissal.

It goes on to add that in the aforementioned Judgment “the worker who had presented the demand for dismissal, seeking its annulment for violating the honor, privacy and dignity or, secondarily, its unfairness, the dismissal was declared appropriate, and in supplication it was confirmed considering that the installation of the cameras covered the trial of proportionality to justify its legality and not violation of fundamental rights.

In amparo, the TC denies the amparo taking into account that the camera was located in the place where the labor provision was developed, focusing directly on the box, considering that it has been adequately weighted that the installation and employment of means of capturing and recording images by the company have respected the

right to personal privacy since the installation was a justified measure.

What is decisive is therefore compliance by the employer with the legal provisions in

data protection and worker information that justifies the use of the

recordings to prove the origin of the dismissal.

It is therefore essential the duty of information that in this case is recognized.

The requested party provides the following documentation:

. It provides a document that the claimed party calls the “Conciliation Document”,

although it is not the conciliation act. Actually, it is a document prepared

by the claimant, in which there is a stamp of the General Directorate of

Employment and Training of the Principality of Asturias and a handwritten indication with the

text “Presented in the conciliation act. ***DATE.3…” and two signatures that are not

identify.

In this document, regarding the reasons for the dismissal, the claimant states:

“The referenced voice recordings coming from a security camera

security installed inside the company, are proof of my despair at not being able to

do my job well because of the lack of training in this regard”.

“That same camera records the conversation with a client who told me that I was

much more competent than the other girl… and I commented to her… that she couldn't perform some

works correctly because of one of the company machines.”

In said document, the claimant requests compensation "for violation of

fundamental rights for making audio recordings from cameras

installed in the workplace.

. Decree of the Labor Court ***JUZGADO.1, dated 06/01/2021, in which the

approves the conciliation reached between the parties. This Decree indicates that the

claimant filed a dismissal claim against the claimed party on the date

***DATE.4, and that the claimed party acknowledges the unfairness of the dismissal.

SIXTH: On 06/27/2022, a resolution proposal was formulated in the sense

following:

1. That the claimed party be penalized for a violation of Article 6 of the GDPR,

typified in Article 83.5.a) of the GDPR, and classified as very serious for the purposes of

prescription in article 72.1.b) of the LOPDGDD, with a fine of 6,000 euros (six

a thousand euros).

2. That the claimed party be imposed, within the term to be determined, the adoption of

the necessary measures to adapt their actions to the regulations for the protection of

personal data, with the scope expressed in the Fundamentals of Law of the

resolution proposal.

SEVENTH: On 08/08/2022, a written statement of allegations to the proposal of

resolution prepared by the claimed party, in which, basically, it reproduces the

arguments set forth in their allegations at the opening of the proceeding, some of

literally, to request the file of the procedure again. Besides what

expressed in his allegations at the opening of the proceeding, the defendant

makes the following considerations:

. None of the data that is said to be captured by the audio has been used, beyond

from a conversation with a client, which was learned through other means.

. The reference to the conversation is only credited by a whatsapp. However, bliss

conversation could not be heard by anyone, so it does not exist to the

effects of the procedure. The conversation was obtained by the interlocutor (the client),

who was the one who communicated its content. The fact that the conversation

appears in the dismissal letter does not presuppose that it was known

by an audio recording and since this recording does not exist, you cannot continue

maintaining that it was captured by the cameras. Nor has the complaining party

heard or seen the recording because it does not exist.

. The procedure does not prove that there was an audio recording containing

personal information.

. The dismissal was unfair and it is not true that it was caused by the content of the

voice recordings from the video surveillance system, it was only one of the

essential aspects contained in the dismissal letter.

. "…audio basically refers to the sound emitted by the machine to accredit the

bad manipulation of the same, which will be accredited at the time by means of the

timely expert evidence.

. The instructor follows the dictation of the complaint, despite the fact that the complaining party knew

the recording system.

. The AEPD is intervening in a labor conflict without any justification and without

Clarify which protected data has been violated.

. Had the recording existed, its purpose would have been to obtain the sound of the

machines due to their mishandling.

. No audio has been used for the adoption of a disciplinary dismissal.

Of the actions carried out in this procedure and of the documentation

in the file, the following have been accredited:

PROVEN FACTS

1. The claimed party is responsible for the video surveillance system installed in the

place where it develops its economic activity, ***ADDRESS.1.

2. The complaining party provided services as an employee of the responding party. Such

Services were provided in the premises where the system is installed.

video surveillance outlined in the First Proven Fact.

3. In relation to the video surveillance system outlined in the Proven Fact

First, the Respondent provided the Complainant with two documents

notices with the labels “Inform workers about the installation of

cameras (Labor Control)” and “Informative Manual on the use of security systems

video surveillance".

In the first of them, which was delivered to the claimant on ***DATE.2,

the installation of the surveillance camera is communicated "for the purposes: to guarantee

the safety of workers, customers, users and all those who

attend the interior of the company's facilities and to carry out a control of

work performance of the workers of the company, during the development of the

characteristic functions of his position. In the same document it is added "that the

information obtained and stored by recording system will be used

exclusively for the purposes of prevention, security, work performance control and

protection of people and goods that are in the establishment or installation

subject to protection”.

The document "Informative Manual on the use of video surveillance systems", in the

containing the handwritten signature of the complaining party, includes, among other things, the

following information:

“The use of cameras or camcorders for security purposes, implies in any case the

capture, recording and storage of images that may contain character data

staff.

Capture or recording may consist of an image system, associated or not with the

voice pickup.

Both the physical image and the voice of people constitute personal data…”.

. The claimed party, in its response to the claim transfer process,

stated to this AEPD that the video surveillance system described in the Fact

Tested First it has sound capture, as well as image capture.

In this same response, the claimed party refers to the recording of a

conversation held by the complaining party with "the clientele".

. Dated ***DATE.1, the complaining party served the complaining party with a letter

through which the termination of the employment relationship is communicated (dismissal letter).

FUNDAMENTALS OF LAW

Yo

Competence

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

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

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: "Procedures

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

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

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures".

The image and voice are personal data

II

The physical image and voice of a person, according to article 4.1 of the GDPR, are a

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

4.2 of the GDPR defines the concept of "processing" of personal data.

The images and voice captured by a system of cameras or video cameras 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 complaining party, who served as an employee in the company of the complaining party

claimed, and of the natural persons who come as clients to the establishment of

said company, open to the public) carried out through the system of

denounced video surveillance is in accordance with the provisions of the GDPR.

II

Infringement

Article 6.1 of the GDPR establishes the assumptions that allow the use of

processing of personal data.

The permanent implantation of a system of video cameras for reasons of

security has a legitimate basis in the LOPDGDD, the explanatory statement of which indicates:

“Together with these assumptions, others are included, 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 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 treatment of images through systems of cameras or video cameras

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

facilities.

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

Employer data obtained through camera or video camera systems will be

submits to the provisions of article 89 of this organic law”.

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

labor, Royal Legislative Decree 1/1995, of 03/24, is taken into account, which approves

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

notes:

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

to verify compliance by the worker with his labor obligations and duties,

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

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

The permitted surveillance and control measures include the installation of

security cameras, although these systems should always respond at first

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

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

job duties.

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

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

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

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

that employers can process the images obtained through security systems

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

workers or public employees provided for, respectively, in article 20.3

of the Workers' Statute and in the civil service legislation, provided that

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

same.

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

sets the following:

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

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

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

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

sound recording in the workplace will be allowed only when relevant

risks to the safety of facilities, goods and people derived from the activity

that it takes place in the workplace and always respecting the principle of proportionality,

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

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

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 conversations between workers or between them and customers is not justified for the verification of compliance by the worker with his obligations or duties.

In a Judgment dated 04/10/2000 (2000/98), issued in rec. num. 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 the art. 20 LET, attributes to the employer, among other powers, that of adopting the measures that deems more appropriate surveillance and control to verify the worker's compliance with their labor obligations (art. 20.3 LET). But this faculty must be produced in any case, As is logical, within due respect for the dignity of the worker, as we expressly It is reminded by the labor regulations (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 in the framework of the relationship

labor, since this cannot imply in any way the deprivation of such rights for those who serve 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 develops within an organization which reflects other constitutionally recognized rights in arts. 38 and 33 CE and that It imposes, according to the assumptions, the necessary adaptability for the exercise of all of them...

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

affirm that the workplace is not by definition a space in which the

workers' right to privacy, in such a way that the conversations that

maintain workers with each other and with customers in the performance of their work activity

They 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

private sphere of the worker, that in the workplace it must be understood limited to the

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

places where work is carried out...

…Such a statement is rejectable, since it cannot be ruled out that also in those

places of the company where the work activity is carried out may produce

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

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

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

workplace in question, which justifies 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, 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 circumstances set out that

allows classifying business action as an illegitimate intrusion into the right to privacy

from the workers. It will be necessary, then, to attend to the concurrent circumstances in the supposed

concrete to determine whether or not there is a violation of art. 18.1 EC.

…its limitation [of the fundamental rights of the worker] by the powers

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

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

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

sacrifice 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 the indispensable and strictly

necessary to satisfy a business interest deserving of guardianship and protection, in a manner

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 those more aggressive and

affective. It is, ultimately, 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... fits in the assumption

that occupies us with 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 devices

for capturing and recording 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 economic transactions of some importance 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 short, the implementation of the listening and recording system has not been in this case in accordance with the principles of proportionality and minimum intervention that govern modulation of fundamental rights due to the requirements of the interest of the organization business, since the purpose pursued (to provide extra security, especially in the face of eventual customer claims) is disproportionate to the sacrifice that 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 given 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 and record the private conversations that the 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 GDPR. We will highlight the principle of data minimization contained in article 5.1.c) of the GDPR that provides that personal data shall 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. 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 at the time of

subsequent treatment carried out on them.

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

proceed to their deletion.

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

that the installed camera or camcorder system cannot obtain images

affecting the privacy of employees, making it disproportionate to capture

images in private spaces, such as changing rooms, lockers or rest areas

of workers.

Video surveillance obligations

IV.

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

video surveillance, to comply 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 cannot reasonably be achieved by

other means, recital 39 of the GDPR.

2.- The images obtained cannot be used for a subsequent 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 GDPR, and 22 of the LOPDGDD.

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

a “layered information” system.

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

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

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

processing of personal data.

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

visible and must be provided in advance.

Second layer information should be easily available in one place

accessible to the affected person, 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

other elements of article 13 of the GDPR.

4.- Images of the public thoroughfare 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

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

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

That is, cameras and camcorders installed for security purposes may not be

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

it is impossible to avoid it due to their location. And in such a 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 admitted.

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

surroundings, adjoining buildings and vehicles other than those that access the space

guarded.

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

consent of their owners, or, where appropriate, of the people who are in them

find.

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

changing rooms, lockers or rest areas for workers.

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, property or facilities.

In this second case, they must be made available to the authority

competent authority within a maximum period of 72 hours from the knowledge of the

recording existence.

6.- The controller must keep a record of processing activities

carried out under his responsibility in which the information to which he makes

reference article 30.1 of the GDPR.

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 security measures.

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 to be the destruction, loss or accidental alteration or

unlawful transfer of personal data, stored or otherwise processed, or the

communication or unauthorized access to said data.

9.- When the system is connected to an alarm center, it can only be

installed by a qualified private security company

contemplated in article 5 of Law 5/2014 on Private Security, of April 4.

The Spanish Data Protection Agency offers through its website

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

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

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 at the

section "Guides and tools").

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

free tool Facilitates (in the "Guides and tools" section) that, through

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

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

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

indicative security considered minimum.

V

administrative infraction

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

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

related to sound recording.

It is not disputed 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 among the data processing carried out is the collection and

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

It is proven in the proceedings, likewise, that said installation is carried out with

safety and labor control purposes.

For this reason, on ***DATE.2, the claimed party communicated to the party

claimant the installation of the surveillance camera “for the purposes: to guarantee the safety of workers, customers, users and all those who attend the interior of the company's facilities and to carry out a control of work performance of the workers of the company, during the development of the characteristic functions of his position. In the same document delivered to the party claimant, in which his handwritten signature and the indicated date appear, also handwritten, it is added "that the information obtained and stored through the recording will be used exclusively for purposes of prevention, security, control of work performance and protection of people and goods that are in the establishment or installation subject to protection”.

It is on record that the claimant was provided with a document labeled "Manual information on the use of video surveillance systems”, which includes, among other things, the following information:

“The use of cameras or camcorders for security purposes, implies in any case the capture, recording and storage of images that may contain character data staff.

Capture or recording may consist of an image system, associated or not with the voice pickup.

Both the physical image and the voice of people constitute personal data…”.

This is the only information provided to the complaining party about the recording of sounds, which is not conclusively presented (“may consist”; “associated or not”)

so that the interested party can be certain about the capture and recording of

personal data related to the voice of the workers.

In its statement of allegations at the opening of the proceeding, the claimed party indicates

that the complaining party admits having been aware of the installation of the system

of video and voice in the document that it provides with said allegations and that

called “Reconciliation Document”. However, in this document, prepared

by the complaining party, it only refers to the recording of a

conversation with a client through the aforementioned system, but it does not refer

any to the specific fact of having had prior and certain knowledge of the installation

of a sound recording system.

In addition, the claimed party does not provide sufficient justification for these treatments.

of data (sound recording), limiting itself to presenting the capture of sounds

as the exercise of the employer's right to "establish the measures that he deems

more timely monitoring and control to verify compliance by the worker

of their labor obligations and duties”.

The claimed party does not take into account the limits set forth in article 20.3 of the Law

the Workers' Statute (LET); what is established in article 89.3 of the

LOPDGDD, which admits the recording of sounds only when they are

relevant risks and respecting the principles of proportionality and intervention

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

recording conversations between workers or between them and customers is not justified

for the verification of compliance by the worker with his obligations or duties.

In response to the allegations made by the defendant regarding the

possibilities in terms of adopting surveillance measures attributed to the

entrepreneur his power of direction, it is interesting to highlight some of the aspects

declared in the Judgment of the Constitutional Court dated 04/10/2000, reviewed

in the Foundation of Law III:

"...this power must occur in any case, as is logical, with 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 the workers maintain with each other and

with clients in the performance of their work activity are not covered by art.

18.1…".

"…its limitation [of the fundamental rights of the worker] by the powers

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

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

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

sacrifice 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 the indispensable and strictly

necessary…".

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

listening and recording equipment, given that the company already had other

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

The claimed party states that the images captured by the

video surveillance made it possible to demonstrate that the complaining party misused

the company's machinery and caused loss of material and time, which led to

interest in activating sound recording for further monitoring

exhaustive to the claimant, as a company worker.

It does not explain, on the other hand, what the recording of conversations between the

complaining party and clients, in order to prove those circumstances, which do not

contribute the mere recording of images, so that it is not sufficiently estimated

substantiated the activation of the sound recording system referred to in the

claimed part. This is in the event that the events occur as indicated.

by the defendant, who has not provided any evidence in this regard. What does exist is

that there was a recording of a conversation between the complaining party and a

customer.

Nor has it provided any proof of the circumstances that

allegedly determined the collection of voice data from the complaining party. Neither

Even such circumstances were asserted against the claim for dismissal

unfair.

Faced with the opening of the procedure, the defendant emphasizes, on the other hand, that

the audio recording was carried out in accordance with the provisions of article 89

of the LOPDGDD given that said recording was not made in places intended for

rest or in places where private conversations took place. However, not

takes into account the claimed party that this article, beyond the prohibition of

use these video surveillance and sound recording systems in "places

intended for the rest or recreation of workers or public employees,

such as changing rooms, toilets, dining rooms and the like", expressly and with character

In general, it establishes the submission of such systems to the legal framework and with the limits

inherent to it, already indicated above (those provided for in article 20.3 of

the Workers' Statute Law (LET); what is established in article 89.3 of the

LOPDGDD; and the doctrine of the Constitutional Court, which does not admit the recording of

conversations between workers and customers to verify compliance by

the worker of his obligations or duties). This implies that it cannot be understood

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

as claimed by the defendant.

Also in his statement of allegations at the opening of the proceeding, the party

claimed invokes a Constitutional Court Judgment 39/2016, of

03/03/2016, in which the amparo appeal filed by a person is dismissed

who was dismissed based on images captured by a security camera

video surveillance. It is, however, a case in which audio is not captured and in

which duly justified the proportionality of the measure adopted by the

employer, taking into account the concurrent circumstances in the analyzed case (“the

filming was confined to the observation of the space in which the box was located

register, examining its handling by the employees having been warned from

substantial mismatches in its accounting some time ago”).

Subsequently, in its pleadings to the resolution proposal, the party

The defendant denies that there is any audio recording, despite the fact that in its

earlier writings acknowledged such existence and that the repeated audio recording

is expressly cited in the dismissal letter provided to the proceedings by the party

claimant.

Specifically, in its response to the transfer process, the party claimed

admits that the system has audio capture and that this option was activated

to follow up on the complaining party. In the same writing it is done

reference to the complaints that the complaining party expresses to the clientele about the state

of the machinery (after warning about the misuse of the machinery that performs the

complaining party and admitting the activation of the audio, it is indicated: "In the following days

another fact is observed, the worker complains to the clientele about the machinery of the

company…").

The mere fact of activating the sound recording already implies in itself a collection

of personal data related to the voice of the complaining party that requires a database

legitimate to carry it out.

In addition, in the dismissal letter prepared by the claimed party it is indicated

expressly the following:

"4. Finally, also discovered in the recordings reviewed yesterday, it was

listen to a conversation on March 4, 2022, in which you complain to a

client about the state of the machinery…".

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

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

intended video surveillance, for the control of compliance by the complaining party of

their job obligations and duties. It is taken into account that the voice recording

It represents a further intrusion into privacy.

Lastly, it should be noted that this conclusion is in no way affected by the fact that the party

claimed will accept as unfair the dismissal of the claiming party, without making

worth repeat recording. The determining factor for the purposes of this proceeding

is that the processing of the complaining party's voice data was carried out by the

claimed party without any legal basis that legitimizes said data processing.

Therefore, it is considered that the claimed party carried out data processing without

have a legitimate basis, contrary to the provisions of article 6 of the GDPR, which

that supposes the commission of an infraction typified in article 83.5 of the RGPD, which

provides the following:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 20,000,000 or,

in the case of a company, an amount equivalent to a maximum of 4% of the

total annual global business volume of the previous financial year, opting for

the highest amount:

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

consent in accordance with articles 5, 6, 7 and 9;".

For the purposes of the limitation period for infringements, the infringement indicated in the

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

which states that:

"Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that

a substantial violation of the articles mentioned therein and, in particular, the

following:

b) The processing of personal data without the fulfillment 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 GDPR establishes:

"Each control authority will have all the following corrective powers

indicated below:

(...)

d) order the person in charge or person 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 in accordance with article 83, in addition to or instead of

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

particular case".

According to the provisions of article 83.2 of the GDPR, 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 GDPR, based on the facts

exposed and without prejudice to what results from the instruction of the procedure, it is

considers that the sanction that should be imposed is an administrative fine.

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

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

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

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

section k) of the aforementioned article 83.2 GDPR.

The following graduation criteria are considered concurrent as aggravating factors:

. Article 83.2.b) of the GDPR: "b) intentionality or negligence in the infringement".

The installation of an audio recording system and its use to record the

conversations that the complaining party could have had with other people

It is done at the initiative of the claimed party, intentionally.

. Article 83.2.d) of the GDPR: "d) the degree of responsibility of the controller or the

processor, taking into account the technical or organizational measures that

applied by virtue of articles 25 and 32".

The claimed party does not have adequate procedures in place for action in

the collection and processing of personal data, in what refers to the

collection and processing of personal data relating to the voice of the employee

in your company, so that the violation is not the result of an anomaly in the

operation of these procedures but a defect in the management system of the

personal data designed by the person in charge.

Likewise, the following circumstances are considered mitigating:

. Article 83.2.a) of the GDPR: "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

damages they have suffered".

. The number of interested parties: the use of the video surveillance system to

labor control affects only the complaining party, as it is the only

a worker of the company at the time the events take place.

. Article 76.2.b) of the LOPDGDD: "b) The link between the offender's activity and the

processing of personal data".

The scarce connection of the claimed party with the performance of treatment of

personal data, considering the activity carried out.

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

the circumstances of the case, such as the financial benefits obtained or the losses

prevented, directly or indirectly, through the infringement".

. The status of microenterprise of the claimed party, which develops its activity

business as private

. The low volume of data and processing that constitutes the object of the

proceedings.

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

Violation of article 6 of the GDPR is 6,000 euros (six thousand euros).

It should be noted that the defendant has not made any claim against

the factors and graduation criteria set forth.

VII

Measures

Considering the declared infringement, it is appropriate to impose the person responsible (the party

claimed) the adoption of appropriate measures to adjust its performance to the

regulations mentioned in this act, in accordance with the provisions of the aforementioned article

58.2 d) of the GDPR, according to which each control authority may "order the

controller or processor that the processing operations are

comply with the provisions of this Regulation, where appropriate, in a

certain manner and within a specified period…".

The text of the resolution establishes which have been the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of data, from which it is clearly inferred what are the measures to adopt, without prejudice that the type of procedures, mechanisms or concrete instruments for implement them corresponds to the sanctioned party, since it is responsible for the treatment who fully knows its organization and has to decide, based on the proactive responsibility and risk approach, how to comply with the GDPR and the LOPDGDD.

However, in this case, regardless of the foregoing, it is agreed to require the responsible so that, within the term indicated in the operative part, it proves that proceeded to suppress the capture of sounds by the object video surveillance system of the performances.

It is noted that not meeting the requirements of this body may be considered as an administrative offense in accordance with the provisions of the GDPR, classified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the opening of a subsequent administrative sanctioning procedure.

Therefore, in accordance with the applicable legislation and assessed the criteria of graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE B.B.B., with NIF ***NIF.1, for a violation of Article 6 of the GDPR, typified in Article 83.5.a) of the GDPR, and classified as very serious to effects of prescription in article 72.1.b) of the LOPDGDD, a fine of 6,000 euros (six thousand euros).

SECOND: REQUEST B.B.B., within a month, counted from the notification of this resolution, adapt its action to the regulations of protection of personal data, with the scope expressed in the Basis of Law VII, and justify before this Spanish Data Protection Agency the

attention to this requirement.

THIRD: NOTIFY this resolution to B.B.B..

FOURTH: Warn the sanctioned party that he must enforce the sanction imposed

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

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

Common of Public Administrations (hereinafter LPACAP), within the payment period

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, by means of its income, 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, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date 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 or immediately following business month, and if

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

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

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

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process 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 reversal before the

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

count 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 for in article 46.1 of the

referred Law.

Finally, it is noted 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 through

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

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

web/], or through any of the other registries 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 proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-120722

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es