 File No.: EXP202205820

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 05/18/2022 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 he has been working since 2019 for a company of the

that the claimed party is responsible and that in the place where it provides its services

a video surveillance camera associated with an alarm is installed, which is

uses as a means of labor control of his job, capturing images and

audio, without having been previously informed of the processing of your data linked to

said camera.

He states that he has learned of the audio capture by said video surveillance system

on 03/24/2022, on the occasion of a WhatsApp conversation held with the

requested party, in which the latter states that it is listening through the

camera.

It also states that the work computers have installed a

application for remote computer access by the claimed party (“In

company computers, whose work is in a shared folder

so that we can access both, it has an application installed (...) to be able to

remotely access and take control of the computer that I use, when for said

end could connect to yours.”).

Provides images of the location of the camera, of the remote control program

installed on the company computer (this is an image of the screen of a

computer showing a remote access application message

indicated by the complaining party with the text “iPhone of… -name of the party

claimed- (***PHONE.2) is connected to your computer”) and screenshots

of a mobile device in which you can see the WhatsApp messages sent

by “***GROUP.1”. These messages indicate:

. “***GROUP.1”: “What do you have in the background? Why is there no music?

. You: "And this?"

. "***GROUP.1": "Because I entered the camera and the news was being heard"

The information that the complaining party provides about the complained party includes,

In addition to the name and ID number, the following data:

. Web page: “***URL.1”.

. Email: “***EMAIL.1”.

. Mailing address: “***ADDRESS.1”.

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,

by writing addressed to "***GROUP.1", to the address "***ADDRESS.1", so that

proceed to 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 delivered by the Postal Service on date 05/31/2022, at the indicated address, and it is recorded received by C.C.C., with DNI ***NIF.2, according to the indications outlined in the acknowledgment of receipt in the file.

In this procedure, the requested party was required to provide information on the video surveillance installed in the referred premises, detailing specifically if the The purpose of this system is labor control, and on the audio training by the same, plus image; as well as information about the installation in the computers of the company of an application to access remotely and if this access is made for the purpose of labor control.

The period of one month granted for the claimed party to respond to the The claim elapsed without any writing being received by this Agency.

THIRD: On 07/19/2022, in accordance with article 65 of the LOPDGDD, The claim presented by the complaining party was admitted for processing.

FOURTH: On 11/04/2022, the Director of the Spanish Protection Agency of Data agreed to initiate disciplinary proceedings against the claimed party, in accordance with the provisions of articles 63 and 64 of the LPACAP, for the alleged violation of the Article 6 of Regulation (EU) 2016/679 (General Regulation for the Protection of Data, hereinafter GDPR), typified in article 83.5.a) of the aforementioned Regulation; and classified as very serious for the purposes of prescription 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 5,000 euros (five thousand euros).

Likewise, it was warned that the accused infringement, if confirmed, may lead to the

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

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/23

the LPACAP, the claimed party submitted a brief of allegations in which it requests that

the nullity of the procedure is agreed or, secondarily, that the

actions to the information request process.

As grounds for its petition, the respondent denies that it was given

reliable transfer of the claim that gives rise to the procedure, procedure to be

makes reference in the Second Antecedent, indicating that he has had knowledge of

said claim with the notification of the beginning of the disciplinary procedure.

It understands that this circumstance infringes what is established in the LPACAP, in relation to

the essential procedures that must be substantiated in a procedure with the purpose of

to prevent the interested party from suffering defenselessness; and the requirement to notify the act as

necessary requirement for its effectiveness.

In this regard, it points out that notifications presenting deficiencies must

considered unsuccessful, cause defenselessness and lead to the nullity or voidability of the

act that they contain for violation of fundamental rights and for having

dispensed with the entire procedure.

For this reason, the claimed party requested a complete copy of the file; what do you know

sent the request for information that "allegedly" was notified, of which

the file brings cause; and a copy of the proof of sending and receiving said

notification.

In this statement of allegations, the claimed party indicates as address for the purposes of notifications the postal address located in "***ADDRESS.1". between the data personal information provided, in addition to the postal address, the line number is indicated phone number “***PHONE.1” and the email address “***EMAIL.1”.

SIXTH: By writing dated 12/15/2022, which was notified on 12/19/2022, it is sent to the claimed party a copy of the actions included in this procedure, which includes the letter of transfer of the claim addressed to "***GROUP.1" that is mentioned in the Second Antecedent and the proof of its delivery.

On the occasion of the remission of the copy of the proceedings, the party was granted demanded a new period of ten business days so that he could present allegations at the opening of the procedure, provide as many documents as you deem timely and formulate test proposal.

In addition, it was warned about the provisions of article 53 "Rights of the interested party in the administrative procedure" of the LPACAP, which recognizes those interested in the procedure the right to know, at any time, the status of the processing and to formulate allegations, use the means of defense admitted by the Law Legal, and to provide documents at any stage of the procedure prior to the hearing process, which must be taken into account when drafting the proposal resolution.

Making use of this new term granted to formulate allegations, dated 12/26/2022 a letter is received from the claimed party requesting that the resolution agreeing the nullity of the disciplinary procedure or, secondarily, the

retroaction of the procedure at the time of the information request.

It reiterates its previous allegations, pointing out that the documentation provided proves

that the request for information in question was addressed to "***GRUPO.1" and not to "B.B.B.".

The claimed party understands that this notification cannot be deemed valid,

given that "***GROUP.1" lacks legal capacity and cannot be interested in the

procedure.

SEVENTH: On 01/05/2023, it was agreed to open the testing period with the practice

of the following:

1. The claim filed by the

complaining party and its documentation, the documents obtained and generated during

the phase of admission to processing of the claim.

2. Likewise, the allegations to the agreement to start the

referenced disciplinary procedure formulated by the claimed party.

3. It was agreed to incorporate the following information and/or documentation into the actions:

a) Result of the search carried out on the Internet with the Google search engine and the criteria

search “B.B.B.”.

The first page of search results includes links, among others, to the

websites “linkedin.com”, “pinterest.es”, “infojobs.net”, “expansión.com” and

“eleconomista.es”.

In the information associated with the link to "linkedin.com" that appears on this page of

results is indicated “(…)”.

It is also verified that the claimed party appears as an individual entrepreneur or

autonomous in the directories of the websites “expansión.com” and “eleconomista.es”.

b) Information (public profile) available on “B.B.B.” on the website “linkedin.com”.

In the "Experience" section it is indicated: "(...)".

c) Information (public profile) available on “B.B.B.” on the website “infojobs.net”.

In this profile (“updated 2018”), the claimed party is presented as “(…)”.

d) Result of the search carried out on the internet with the Google search engine and the criteria

search “***GROUP.1”.

The first page of search results includes links to the website

"***URL.1" and the profiles of "***GRUPO.1" on the social networks "Facebook" and

"Instagram". In the data that is related to "***GROUP.1" appears the address

located in “***ADDRESS.1” and the telephone line number “***PHONE.2”.

e) Information available on the website "***URL.1", section "Contact".

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

As contact details of "***URL.1" a postal address is mentioned

("***ADDRESS 1"),

and

“***PHONE.2”) and an email address (“***EMAIL.1”).

("***TELEPHONE 1"

lines of

telephony

two

f) Information available on “***GROUP.1” on the website “linkedin.com”.

It presents itself as a “(…)” company, and includes information about its website

(“***URL.1”), headquarters (“***PROVINCE.1”), type (“Own company”), main location (“***ADDRESS.1”) and employees (“B.B.B., (…) in ***GROUP.1”). includes messages inserted by the person quoted with the text "personal search".

EIGHTH: On 02/06/2023, a resolution proposal was formulated in the sense following:

1. That the claimed party be penalized for a breach 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 5,000 euros (five thousand euros).

2. That the claimed party be required so that, within the term to be determined, adopt the necessary measures to adapt its actions to the regulations of protection of personal data, with the scope expressed in the Basis of Law VIII of the proposed resolution.

NINTH: The proposed resolution outlined in the Eighth Antecedent was notified to the claimed party on 02/07/2023, granting him a term to make allegations.

On 02/16/2023, a written statement of allegations to the resolution proposal was received in which the claimed party once again requests that the nullity of the actions or, in a subsidiary way, the retroaction of actions to the phase is agreed of admission to processing of the claim, at the time of the transfer of the claim to the person responsible, or the procedure is archived. In this writing it is put reveal the following:

1. In relation to the nullity of the proceedings, he almost literally reiterates his previous allegations in this regard and adds that the motion for a resolution recognizes that the process for transferring the claim was addressed to "***GRUPO.1" and not to "B.B.B."

2. The principle of classification is violated, since it is false that the system of

video surveillance collects and stores personal data relating to the voice of employees and

third parties, concluded in the motion for a resolution based on a WhatsApp message

provided by the complaining party, based on which it understands that the principle of

presumption of innocence.

And adds:

"Having said this, it is flatly false that I have any video surveillance system in my premises that

can collect and store data related to the voice of employees and third parties, since in

In relation to listening to audio, the only thing I have contracted are alarms or security systems.

alerts that incorporate microphones that allow audio to be heard, but not recorded or logged

these audios, all for the purpose of being able to verify any incident...

For all these reasons, if my video surveillance system is the only thing you have contracted in relation to the

audio listening are alarms or alert systems that incorporate microphones that allow

listen to audio, but not record or record these audios, you would not be committing the offense

that is charged to me."

As a document accrediting his statements, he says to provide the signed contract

with a security company. However, it is an unsigned document and in

which does not even contain the data of the party claimed as a client of the company

that is quoted

3. Considering that the facts are not true, the proposed sanction is contrary to the

principle of proportionality, as it is not related to the objective circumstances and

concurrent subjective, nor does it pay attention to the seriousness and transcendence of the fact, the

background of the offender and his status as a repeat offender, or the intent and

damages caused.

4. The principles of presumption of innocence and "indubio pro reo" are violated when

base the sanction on the screenshots provided by the complaining party,

relating to a conversation allegedly held with the claimed party, which

that denies Thus, it considers that it is appropriate to apply the provisions of article 89.1.b) of the

LPACAP, which orders the filing of proceedings when the facts are not

accredited

According to the defendant, in this proceeding they have not been incorporated into the

file the appropriate evidence for the correct and complete

determination of the facts and of the persons responsible for them,

limited to making a generic statement of guilt in relation to some

acts that have not been committed by the accused in the form and extent that

they presume, without adequate evidence, made by the taxpayer of the file. AND

warns that the burden of proof corresponds to the acting Administration.

He ends by pointing out that in the event that in the evaluation of the evidence

the slightest shadow of reasonable doubt existed as to the guilt imputed by

divergence between them, as in the present case, would be fully applicable

the general principle "in dubio pro reo", which -as a rule of interpretation of

procedural nature - determines that in case of doubt the file is resolved

sanctioning in the most favorable sense for the presumed offender.

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 carries out its economic activity as an individual entrepreneur,

under the trademark "***GRUPO.1", with professional domicile at

"***ADDRESS 1".

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2. The business premises located at "***ADDRESS.1" have a system of

video surveillance, for which the claimed party is responsible.

3. The claimant has stated that he provides services as an employee of the

claimed party in the place located at the postal address indicated in the Facts

Tested First and Second.

4. The complaining party stated that the video surveillance system described in the

Fact Tested Second has sound pickup, in addition to voice pickup

image.

In this regard, the complainant contributed to the proceedings with screenshots of

a mobile device in which you can see WhatsApp messages that were sent to you

sent by the claimed party ("***GROUP.1"). These messages indicate:

. "***GROUP.1": "What do you have in the background? Why is there no music?

. You: "And this?"

. "***GROUP.1": "Because I entered the camera and the news was being heard"

FUNDAMENTALS OF LAW

Yo

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

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

guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

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".

II

formal issues

In advance, it is deemed appropriate to analyze the formal issues raised

by the party claimed in their pleadings, both at the opening of the

procedure and in relation to the motion for a resolution.

It considers that the procedure is null and void since it was not notified

evidence of the claim in which it originates, of which he became aware with the

notification of the initiation agreement, violating what is established in the LPACAP, in

relation to the essential procedures that must be substantiated in a procedure for

prevent the interested party from suffering defenselessness; and the requirement to notify the act as

necessary requirement for its effectiveness.

The claimed party refers, specifically, to the procedure for forwarding the claim that

It is reported in the Second Antecedent, which was not addressed to "B.B.B.", but to "***GROUP.1", which lacks legal capacity and cannot be interested in the procedure.

In this regard, this Agency understands that the claimed party has been respected all the guarantees of the interested party that the procedural regulations provide and it cannot be said that the incidence indicated in relation to the process of transferring the claim supposes no reduction of said guarantees causing defenselessness.

The indicated notification of transfer of the claim to the person in charge to whom refers to the party claimed in its allegations has to do with the process of admission to processing of the claims received, prior to the agreement of admission of such claims.

In accordance with the provisions of article 55 of the GDPR, the Spanish Agency for Data Protection is competent to perform the functions assigned to it in its article 57, among them, that of enforcing the Regulation and promoting the sensitization of controllers and processors about the obligations incumbent upon them, as well as dealing with claims filed by a interested and investigate the reason for them.

Correlatively, article 31 of the GDPR establishes the obligation of those responsible and those in charge of the treatment to cooperate with the control authority that requests it in the performance of their functions. In the event that they have designated a data protection delegate, article 39 of the GDPR attributes to him the function of cooperate with said authority.

In the same way, the internal legal system, in article 65.4 of the LOPDGDD, has provided for a mechanism prior to the admission for processing of the claims that are formulated before the Spanish Agency for Data Protection, which consists of giving transfer of the same to the data protection delegates designated by the

responsible or in charge of the treatment, for the purposes provided in article 37 of

the aforementioned norm, or to them when they have not designated them, so that they proceed to the

analysis of said claims and to respond to them within a month. In this

Article 65.4 of the LOPDGDD, which regulates the "Admission for processing of

claims", establishes the following:

"4. Before deciding on the admission for processing of the claim, the Spanish Agency for

Data Protection may send it to the data protection delegate that there is, in

appropriate, designated the person in charge or in charge of the treatment or the supervisory body

established for the application of the codes of conduct for the purposes set forth in the

articles 37 and 38.2 of this organic law.

The Spanish Agency for Data Protection may also send the claim to the

responsible or in charge of the treatment when a delegate of

data protection nor adhered to extrajudicial dispute resolution mechanisms.

conflicts, in which case the person responsible or in charge must respond to the claim in

within one month."

According to this regulation, prior to the admission for processing of the claim

that gives rise to this procedure, it was transferred to the person in charge (the

claimed party) to proceed with its analysis, respond to this Agency in

within one month and certify having provided the complaining party with the response

due.

The result of said transfer was not satisfactory, therefore, for the purposes foreseen

in its article 64.2 of the LOPDGDD, it was agreed to admit the claim for processing
presented by means of an agreement that was duly notified to the complaining party,
and not to the claimed party, in accordance with the provisions of article 65.5 of the
LOPDGDD.

This procedure prior to the admission of the claim, according to article 65.4 of the
LOPDGDD previously transcribed, it is an optional procedure, so that
formalized only if this Agency deems it so, without any
legal consequence of the fact that this procedure is not carried out or in case of
that, once attempted, could not have been carried out effectively; nor does it prevent
the claim can be admitted for processing and given the appropriate course. neither are you
circumstances have any bearing on the validity of the possible proceeding
disciplinary action that could be initiated later.

In this case, in addition, the notification of the transfer process, as detailed in the
antecedents of this act, it occurred in a valid and reliable manner at the address in
the one in which the claimed party carries out its activity, the same indicated by said party
as address for notification purposes. The document in question was delivered in that
address by the Postal Service on 05/31/2022.

It is true, as has been pointed out, that the notification was addressed to "***GROUP.1" and not to
"B.B.B." However, in the proceedings it has been proven that the party
claimed operates under the trademark "***GRUPO.1". The claimed party itself
is presented in their public profiles accessible on the websites "linkedin.com" and
"infojobs.net" as "(...) ***GROUP.1" since September 2016.

Also, in his pleadings brief at the opening of the proceeding, he points out the party
claimed as contact information, in addition to the postal address to which the
transfer process, the email address "***EMAIL.1". Both
addresses, postal and electronic, also appear as contact information on the site

website “***URL.1”.

Despite this, the period of one month granted to the claimed party to inform

on the issues raised by the claim and addressing it took place without

that this Agency received any response.

The defendant, in its allegations to the proposed resolution, reproduces its

previous allegations on the nullity of actions for the sending of the notification

of the transfer of the claim to "***GROUP.1", without considering the arguments

above, about which it does not mention.

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 serves as an employee in the company of the 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.

IV.

Infringement

The complaining party bases its claim on two grounds. First of all,

questions that the complained party can access the computer he uses at work,

using an application that allows remote access to the device. Without

However, it is a company computer accessed by the party claimed in

his status as head of the organization. Furthermore, the complaining party

It only refers to access to a shared folder in which they are hosted

company jobs. Thus, from what was provided and stated by the claimant

no indications of infringement are deduced.

The second reason for the claim has to do with the audio capture by the

video surveillance system installed in the workplace of the complaining party and the

legality of the processing of personal data that it entails.

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

processing of personal data:

"1. Processing will only be lawful if at least one of the following conditions is met:

a) the interested party gave his consent for the processing of his personal data for one or

various specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is a party

or for the application at his request of pre-contractual measures;

c) the processing is necessary for compliance with a legal obligation applicable to the

responsible for the treatment;

d) the processing is necessary to protect vital interests of the data subject or of another person

physical;

e) the processing is necessary for the fulfillment of a task carried out in the public interest

or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the user.

responsible for the treatment or by a third party, provided that such interests are not

the interests or fundamental rights and freedoms of the data subject prevail

require the protection of personal data, in particular when the data subject is a child.

The provisions of letter f) of the first paragraph shall not apply to the treatment carried out by

public authorities in the exercise of their functions.

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.

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

labor, 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”.

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

Consolidated Law of the Workers' Statute (LET), whose article 20.3 states:

"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."

In any case, employers must inform in advance, and in a

express, clear and concise, to workers or public employees and, where appropriate, to

their representatives, about this measure (article 89.1 of the LOPDGDD).

Video surveillance obligations

V

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.

Administrative offense. Classification and qualification of the infraction.

SAW

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 relation to sound capture.

The claimed party is the owner and responsible for the video surveillance system denounced and, therefore, the person responsible for the data processing involved in the use of said system. The data processing carried out includes the collection of personal data related to the voice of employees and third parties that can access the premises, which appears to be an establishment open to the public, in view of the image provided by the claimant.

In relation to said system, the complaining party has stated that the system is was installed when he began to serve as an employee of the part claimed, in 2019, "supposedly as a security measure for the premises"; and? has never been informed about the capture of sound or its use for purposes of labor control, which constitutes, in the opinion of the complaining party, a use "for a purpose other than that which is stated to have been installed."

Therefore, the legality of the video surveillance system installed by the party is questioned. claimed in the premises where it carries out its business activity, in relation to the sound capture, which has been duly accredited by the complaining party with the contribution of a WhatsApp conversation in which the claimed party makes reference to their access to the video surveillance system and the sound captured by it.

The claimed party has not provided any justification in relation to the issues

raised by the complaining party, despite the fact that it was expressly required with

occasion of the process of transfer of the claim, which was not answered by that one.

It has limited itself to denying having received that request for information, according to

been exposed in the Fundamentals of Law II.

It has indicated that if it had received that communication it would have provided the

required information. However, he has had occasion, twice, to formulate

allegations at the opening of this disciplinary proceeding, and also in

response to the motion for a resolution, and has not provided information and/or

any documentation relating to the system installed in the establishment in question.

It is interesting to note in this regard that the defendant was asked to prove that they had

informed the workers that the video surveillance system is used for control

and to provide a technical report on said system.

In arranging for sound pickup, the defendant disregards the limits

provided for in article 20.3 of the Workers' Statute Law (LET); it

established in article 89.3 of the LOPDGDD, which admits the collection and recording of

sounds only when the risks are relevant and respecting the principles

proportionality and minimal intervention; nor the doctrine of the Constitutional Court,

already expressed, according to which the "implementation of listening and recording systems" does not

is legitimized, without further ado, by the "mere utility or convenience of the company", which the

"gathering private comments, both from customers and workers" is

outside the business interest and is not justified by the verification of compliance by the

worker from his obligations or duties.

Consequently, it is understood disproportionate the capture of the voice of both the workers and clients of the claimed party for the video surveillance function intended. It is taken into account that the capture of voice supposes a greater intrusion in privacy.

The defendant, in its allegations to the proposed resolution, has stated that it is false that the video surveillance system collects and stores personal data related to the voice of employees and customers, and considers that the screenshot provided by the claimed party does not prove the facts, thus invoking the principles of presumption of innocence and “indubio pro reo”.

However, this Agency considers that the capture of sounds by the indicated security system is accredited by the content of the message sent by the claimed party to the claiming party through Whatsapp, which is outlined in the Fourth Proven Fact. In this message, the claimed party declares to have entered “into the camera” and accessed the sound captured by it (“they heard news").

Moreover, in the same allegations it expressly acknowledges that the system "that has contracted" incorporates microphones "that allow listening to audios".

By not recording or recording audios, the claimed party considers that he is not committing the infraction that is imputed, without considering that the mere capture of audios, even without

to proceed with its recording and conservation, constitutes data processing

personal information that requires a legitimate basis to be able to carry it out,

in accordance with the provisions of article 6 of the GDPR.

Article 4 of the same GDPR defines "processing" in the following terms:

"2) "processing": any operation or set of operations performed on data

personal data or sets of personal data, whether by automated procedures or not,

such as the collection, registration, organization, structuring, conservation, adaptation or

modification, extraction, consultation, use, communication by transmission, diffusion or

any other form of authorization of access, comparison or interconnection, limitation, deletion or

destruction".

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

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

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

provides the following:

Violations of the following provisions will be penalized, in accordance with section

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

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

previous financial year, opting for the highest amount:

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

tenor of 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, 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 fulfillment of any of the legal conditions of the

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

VII

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.

Regarding the infringement of article 6 of the GDPR, based on the facts

exposed, it is considered that the sanction that would correspond to 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 GDPR. Thus

considers, in advance, the microenterprise status of the claimed party,

who develops economic activity as a natural person under the condition of

autonomous entrepreneur.

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

provisions of article 83.2 of the GDPR, which states the following:

"2. Administrative fines will be imposed, depending on the circumstances of each case.

individually, in addition to or in lieu of the measures contemplated in article 58,

section 2, letters a) to h) and j). When deciding to impose an administrative fine and its amount

in each individual case due account shall be taken of:

a) the nature, seriousness and duration of the offence, taking into account the nature,

scope or purpose of the processing operation in question as well as the number of

affected stakeholders and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to alleviate the

damages suffered by the interested parties;

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

of the technical or organizational measures that have been applied by virtue of articles 25 and 32;

e) any previous infringement committed by the controller or processor;

f) the degree of cooperation with the supervisory authority in order to remedy the

infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in particular if the

Controller or processor notified the infringement and, if so, to what extent;

i) when the measures indicated in article 58, paragraph 2, have been ordered

previously against the person in charge or the person in charge in relation to the same

matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or certification mechanisms

approved under article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as

financial benefits obtained or losses avoided, directly or indirectly, through

the offence".

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD,

Regarding section k) of the aforementioned article 83.2 GDPR, it provides:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of Regulation (EU)

2016/679 will be applied taking into account the graduation criteria established in the

section 2 of said article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679 also

may be taken into account:

a) The continuing nature of the offence.

b) Linking the offender's activity with data processing

personal.

c) The benefits obtained as a consequence of the commission of the infraction.

d) The possibility that the conduct of the affected party could have led to the commission of the

infringement.

e) The existence of a merger process by absorption subsequent to the commission of the infraction,

that cannot be attributed to the absorbing entity.

f) The affectation of the rights of minors.

g) Have, when it is not mandatory, a data protection delegate.

h) Submission by the person responsible or in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which there are

disputes between those and any interested party".

In this case, the graduation criteria are considered concurrent as aggravating factors.

following:

. 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 operation

treatment in question as well as the number of interested parties affected and the

level of damages they have suffered".

. The nature and seriousness of the infringement, taking into account that the party

claimant and the rest of those affected (third parties who access the establishment

of the claimed party) are unaware of the data processing that is being

being carried out (sound capture by the video surveillance system) and the

use that will be made of personal data, which affects the ability to

data subjects to exercise real control over their personal data.

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

The negligence appreciated in the installation of video surveillance cameras that

allow the collection of audio in a work environment, without even informing

employees and others affected, and even though these systems have a

special and express regulation that imposes special care on those responsible

in its use.

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

processor, taking into account technical or organizational measures

that they have applied by virtue of articles 25 and 32".

The claimed party does not have adequate action procedures in place

in the collection and processing of personal data, as regards

to the collection and processing of personal data related to the voice of the person

employee in your company, so that the infringement is not the result of a

anomaly in the operation of said procedures but rather a defect in the

personal data management system designed by the controller.

. Article 83.2.g) of the GDPR: "the categories of personal data

affected by the infringement";

Although "Special categories of personal data" have not been affected,

as defined by the GDPR in article 9, the personal data to which they refer

actions (voice of stakeholders) has a particularly

sensitive and increases the risks to your privacy.

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

violation of article 6 of the GDPR is 5,000 euros (five thousand euros).

In view of what is stated in this Legal Basis, it is not true what

indicated by the party claimed in its allegations, according to which the sanction

imposed is not related to the objective and subjective circumstances

concurrent, nor does it attend to the seriousness and transcendence of the fact.

It also refers to the absence of antecedents of the offender and the absence of

damages, but without providing any reasoning that justifies the consideration of

these grading factors.

None of the grading factors considered is mitigated by the fact that

that the claimed entity has not been subject to a disciplinary procedure with

above, this circumstance is alleged by the claimed party to be

considered as a mitigation.

In this regard, the Judgment of the AN, of 05/05/2021, rec. 1437/2020, indicates:

"It considers, on the other hand, that the non-commission of a

previous violation. Well, article 83.2 of the GDPR establishes that it must be taken into account

for the imposition of the administrative fine, among others, the circumstance "e) any infraction

committed by the person in charge or the person in charge of the treatment". It is a

aggravating circumstance, the fact that the budget for its application does not exist

entails that it cannot be taken into consideration, but it does not imply or allow, as it claims

the plaintiff, its application as mitigation".

According to the aforementioned article 83.2 of the GDPR, when deciding to impose a fine

administration and its amount must take into account "any previous infraction committed

by the person responsible." It is a normative provision that does not include the inexistence of

previous infractions as a factor for grading the fine, which must be

be understood as a criterion close to recidivism, although broader.

VIII

possible measures

It is appropriate to impose on the controller the obligation to adopt appropriate measures to

adjust its performance to the regulations mentioned in this act, in accordance with the

established in the aforementioned article 58.2 d) of the GDPR, according to which each authority of

control may "order the person in charge or person in charge of the treatment that the

processing operations comply with the provisions of this Regulation,

where appropriate, in a specified manner and within a specified period…".

The text of this resolution establishes which have been the infractions

allegedly committed and the facts that give rise to the violation of the regulations
of data protection, from which it is clearly inferred what are the measures to
adopt, without prejudice to the type of procedures, mechanisms or instruments
specific measures to implement them correspond to the sanctioned party, since it is the
controller who fully knows his organization and has to decide,
based on proactive responsibility and risk approach, how to comply with the
GDPR and the LOPDGDD.

However, in this case, regardless of the foregoing, this Agency estimates
proceeding to require the person in charge so that within the period determined in the part
device suppresses the capture of sounds by the video surveillance system object 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 same Regulation, and qualified as very
for the purposes of prescription in article 72.1.b) of the LOPDGDD, a fine of

5,000 euros (five thousand euros).

SECOND: REQUIRE B.B.B. so that, 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 VIII, 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 IBAN number: ES00 0000 0000 0000 0000 0000 (BIC/SWIFT Code: XXXXXXXXXXX), opened on behalf of the Spanish Agency for Data Protection in the banking entity CAIXABANK, S.A. Otherwise, it will proceed to its collection in 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

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es