 File No.: EXP202204455

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) dated April 8, 2022

filed a claim with the Spanish Data Protection Agency. The

The claim is directed against B.B.B., with NIF ***NIF.1 (hereinafter, the party

claimed). The reasons on which the claim is based are the following:

1. Installation of security cameras, with notice to workers in the middle of

2021, omitting that said cameras record audio and the establishment's sink, the

which has no door

Indicates that one of the cameras, installed in the year 2020, is located above the

counter, focusing on the entrance, and records the conversations of customers and

Workers. The other camera, installed in January 2021, is located behind the

counter panel, focusing on the warehouse and access to the bathroom (provides images

about the location of the cameras).

You understand that the sound recording is disproportionate and not justified by the

developed activity.

2. The workers were not informed about the use of the system of

video surveillance for labor control or for the purpose of preserving the safety of

people and goods, nor that said system incorporated audio recording.

In addition, the warning sign is not easily visible, not even for the workers

nor for the public, since it is almost covered by the air conditioning unit and

located on one side of the establishment (it is not possible to see it when entering the premises, so

that is not located in a visible place for the clients of the establishment); does not inform about the treatment, the identity of the person in charge and the possibility of exercising the rights recognized to the interested parties; and refers to the previous regulations (Provide a photograph accrediting these circumstances).

3. Workers have access to the recordings made by security cameras. video surveillance, since some are sent to the company's mobile phone, which is permanently in the establishment available to all workers, breaching the regulations on the conservation of recordings.

The complainant also points out that the person in charge sent links to the recordings through the company's WhatsApp group, allowing all

workers access them.

Provide a video accrediting the sending through WhatsApp of a link to a recording from the video surveillance system object of the claim. The recording in question includes sound (the voices of the people are heard captured in said recording, workers and clients).

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 04/20/2022 as stated in the acknowledgment of receipt in the file.

On 19/25/2022, in its response to the transfer of the claim, the party Claimant reports the following:

. The system has two cameras that are inside the premises and only record the same. It is stated that the images are stored for 30 days in a camera and 3 hours in another.

It provides images of the field of vision of the cameras, in which it is not appreciated that capture the restroom indicated in the claim.

. Attach photographs of the informative poster displayed in the establishment.

It is verified that it is located in the same place indicated in the claim, although its content has been modified to be consistent with the data protection regulations. It is verified that instead of informing about the identity of the person in charge refers to the commercial name of the establishment; informs about the exercise of rights and cites a regulation that is not in force.

. It is indicated that the cameras do not record sound and to accredit it, a screenshot of the mobile application that manages the system in which the handwritten indication "disconnected" in the option corresponding to the sound, which can be reactivated at any time quickly and easily, just by scroll tab.

. A document is provided with the signature of the complaining party, to justify that it has informed the workers of the policy for the use of the devices made available available to the workers by the employer, together with another letter of confidentiality that the workers also sign, indicating that the

worker authorizes the display of his image in the internal security circuits

installed by the company.

In none of these writings is it expressly stated that one of the purposes of the

video surveillance system of the establishment is the labor control of the

workers.

. Finally, it is stated that the system is only accessed by the owner, who is responsible for the

treatment through your mobile with username and password.

On the other hand, it does not provide any information in relation to the work chat and the

referral to it of videos recorded by the security system, such as the one

contributes with the claim, despite having been required to do so in the application for

information that was sent to you.

THIRD: On June 16, 2022, in accordance with article 65 of the

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

FOURTH: On 08/05/2022, by the General Subdirectorate of Data Inspection

information related to the claimed party is accessed in “Axesor” (“Informe

monitors"). (…).

FIFTH: On 08/10/2022, the Director of the Spanish Agency for the Protection of

Datos agreed to initiate disciplinary proceedings against the claimed party, in accordance with the

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

Articles 13 and 6 of the GDPR, typified in articles 83.5.b) and 83.5.a) of the same

Regulation, and classified as very serious for the purposes of prescription in articles

72.1.h) and 72.1.b) of the LOPDGDD, respectively.

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

resulting from the instruction, would amount to a total of 3,000 euros (three thousand euros): 1,000

euros (one thousand euros) for the alleged violation of article 13 of the GDPR and 2,000 euros

(two thousand euros) for the alleged violation of article 6 of the GDPR.

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.

SIXTH: On 08/30/2022, he entered this Agency in writing from the party

claimant by means of which he communicates that he withdraws from the claim that he has given

venue for performances.

SEVENTH: Notification of the aforementioned initiation agreement in accordance with the established regulations

in the LPACAP, a written statement was received from the claimed party, in which

requests the file of the procedure. In relation to the facts that have determined

the opening of this disciplinary proceeding, the defendant formulates the

following manifestations:

. The installed video surveillance system has two cameras that do not record

sound.

. With his response to the transfer process, he attached photographs of the

signs warning about the existence of video surveillance and notification

personalized and with acknowledgment of receipt that was made in this regard to the workers.

With its allegations, the claimed party does not provide any document, and requests that

An on-site inspection is carried out to verify the legality of the system.

EIGHTH: On 09/09/2022, a resolution proposal was formulated in the sense

following:

1. That the claimed party be penalized for a breach of article 13 of the GDPR,

typified in article 83.5.b) of the same Regulation, and classified as very serious

effects of prescription in article 72.1.h) of the LOPDGDD, with a fine of 1,000

euros (thousand euros).

2. 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 2,000 euros (two

a thousand euros).

3. 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.

NINTH: The proposed resolution outlined in the Eighth Antecedent was

notified to the claimed party. In said notification, he was granted a term to

make allegations against the proposed resolution, which passed without

this Agency has received any writing.

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

establishment open to the public in which it develops its economic activity.

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

First, the claimed party placed an informative sign on the side of the

establishment, in its upper part, partially covered by an air apparatus

conditioned. Said poster did not inform about the treatment, the identity of the

responsible and the possibility of exercising the rights recognized to the interested parties; and

referred to the previous regulations (provide a photograph accrediting these

circumstances).

Said sign was replaced by another once the claim by the party was known.

claimed. This new poster, which is located in the same place indicated in

the previous paragraph, instead of informing about the identity of the person in charge makes

reference to the commercial name of the establishment; reports on the exercise of

rights and cites a regulation that is not in force.

3. There is a document in the proceedings with the label "Commitment to

confidentiality of employees", arranged by the claimed party so that they are

signed by their employees. In this document, in relation to the system of

video surveillance installed in the establishment, only collects the authorization of the

worker for the visualization of his image in the internal security circuits

installed by the company.

4. The video surveillance system described in the First Proven Fact is managed through

through an application installed on the mobile of the claimed party. This application

allows you to activate or deactivate the option corresponding to the capture and recording of

sound.

5. A video from the video recording system is incorporated into the proceedings.

video surveillance object of the claim that includes sound (the voices of

the people captured in said recording, workers and clients).

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".

II

In advance, it should be noted that article 63.1 of the LPACAP determines that

"Procedures of a sanctioning nature will always be initiated ex officio by

agreement of the competent body", establishing in article 68 of the LOPDGDD

which corresponds to the "Presidency of the Spanish Data Protection Agency,

when appropriate, issue an agreement to start the procedure for the exercise of the

sanctioning power". Thus, for the claiming party to withdraw their claim is

irrelevant and does not imply the filing or completion of the disciplinary procedure

initiated, since it begins and is processed in all its phases ex officio.

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 or of other persons serving as employees of the

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

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

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

IV.

Infringement

Article 12.1 of the GDPR indicates that whoever carries out data processing

personal, such as the capture of images through a system of

video surveillance, must provide the interested parties with the information indicated in the

Articles 13 and 14 of the GDPR.

In order that the duty of information provided for in article 12 of the GDPR is

complies in a concise and understandable manner for the affected party, the aforementioned article 22 of the

LOPDGDD foresees in relation to video surveillance a system of "information by

layers".

In this sense, 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 on the processing of personal data.

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.

It is not necessary to specify the precise location of the video surveillance equipment.

This duty of information will be understood fulfilled by placing a

Information device in a sufficiently visible place, and at least, at the entrances

to monitored areas, whether interior or exterior. In case the space

video surveillance has several accesses must have said hallmark of

video surveillance area in each of them.

This information must be provided in advance -recital 39 of the GDPR-. He

The aim is to make the context of surveillance clear.

On the other hand, article 6.1 of the GDPR establishes the assumptions that allow

consider the processing of personal data lawful.

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."

Video surveillance obligations

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 Corps.

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.

SAW

administrative infraction

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.

In relation to said system, in this case the existence of a cartel

informative that is not located in a sufficiently visible place and does not include all the

first layer information that must be offered to the interested parties, regarding the

identity of the person in charge, the possibility of exercising the rights provided for in the

Articles 15 to 22 of the GDPR and where to obtain more information about the treatment of

personal data, in addition to citing a regulation that is not in force.

It is considered that these facts violate the provisions of article 13 of the GDPR, for

which 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 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:

(…)

b) the rights of the interested parties in accordance with articles 12 to 22; (…)".

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 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:

(…)

h) The omission of the duty to inform the affected party about the processing of their personal data

in accordance with the provisions of articles 13 and 14 of Regulation (EU) 2016/679 and 12 of this

Organic Law".

In addition, the claim is based on the alleged illegality of the video surveillance system

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

in relation to sound recording, which has been duly accredited by the

complaining party with the contribution of a video captured by said system in which

recorded the conversations of workers and customers who were

in the establishment of the person in charge.

There is no record in the proceedings that the person in charge has informed clients and

workers on the collection of their personal data related to the voice of the

interested.

Nor does the claimed party take into account the limits set forth in article 20.3 of

the Workers' Statute Law (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.

Consequently, it is understood that the capture of the voice of both the workers

as clients of the claimed party for the intended video surveillance function

It is not motivated nor does it have legal protection. It is taken into account that the voice recording

It represents a further intrusion into privacy.

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

legitimate basis, violating the provisions of article 6 of the GDPR, which implies the

commission of an offense classified in article 83.5 of the GDPR, which provides

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”.

In relation to the facts constituting these infractions, the claimed party, in

his pleadings at the opening of the proceeding, he has limited himself to denying that

the system captures sounds, despite the verified evidence, such as the option

enabled in the application that manages said system, installed on the device

mobile phone of the claimed party, which allows you to activate or deactivate the capture and recording

of sounds, as well as the video provided by the complaining party, in which the

the voices of workers and customers.

The same can be said regarding the breach of the duty to inform. The part

The defendant reiterates that it has an information poster located inside the

establishment, but does not make any statement in relation to its inadequate

location and with the defects appreciated in the information it contains.

Regarding the information offered to the workers, it again alleges that it

notified the existence of the video surveillance system, but does not accompany any

document other than the one provided with your response to the transfer process of the

claim, in which the workers are not informed about the sound capture.

As stated in the Third Proven Fact, the document referred to by the party

claimed, which is labeled “Employee Confidentiality Commitment,”

in relation to the video surveillance system installed in the establishment,

It only collects the authorization of the worker to display his image in

internal security circuits installed by the company.

VII

Sanction

Article 58.2 of the GDPR establishes:

"Each control authority will have all the following corrective powers indicated to

continuation:

(...)

d) order the person in charge or in charge of processing that the processing operations be

conform to the provisions of this Regulation, where appropriate, of a given

manner 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 section, according to the circumstances of each case

particular".

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 infringements of articles 13 and 6 of the GDPR, it is considered that the

The sanction that corresponds to impose 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, 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 infraction;

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

has:

"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".

The balance of the circumstances contemplated, with respect to the infractions

committed, allows setting the value of the fine at 1,000 euros (one thousand euros) for the

infringement of article 13 of the GDPR and 2,000 euros (two thousand euros) for the infringement

of article 6 of the same Regulation.

VIII

Measures

Considering the infringements declared, 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 actions, as well as compliance with the duty to inform, facilitating the workers the information required by the GDPR and completing the information that is offered through the informative poster installed in the establishment, whose location it should be varied so that it is easily visible.

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 13 of the GDPR, typified in Article 83.5.b) of the GDPR, and classified as very serious to effects of prescription in article 72.1.h) of the LOPDGDD, a fine of 1,000 euros (thousand euros).

SECOND: 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 2,000

euros (two thousand euros).

THIRD: REQUIRE B.B.B. so that, within a month 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

Right VIII of this resolution, and justify before this Spanish Protection Agency

of Data the attention of this requirement.

FOURTH: NOTIFY this resolution to B.B.B..

FIFTH: 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 the LPACAP, within the voluntary payment period established in art. 68 of the

General Collection Regulations, approved by Royal Decree 939/2005, of 29

July, in relation to art. 62 of Law 58/2003, of December 17, through its

income, indicating the NIF of the sanctioned and the number of the procedure that appears in

the heading of this document, in the restricted account no. ES00 0000 0000

0000 0000 0000, opened in the name of the Spanish Data Protection Agency 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

938-120722

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es