 File No.: EXP202102762

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Dated September 20, 2021, entered this Agency

Spanish Data Protection, a document presented by D. A.A.A. (hereinafter the

claimant), through which he makes a claim against D.B.B.B. with NIF ***NIF.1 (in

hereinafter, the claimed), for the installation of a video surveillance system installed in

Cafeteria

STREET

*** ADDRESS.1, there being indications of a possible breach of the provisions of the

data protection regulations.

*** SHOPPING CENTER.1,

***CAFETERIA.1 of C.C.

The claimant states that “There is a video surveillance camera installed on the premises that

it also captures audio and is not signposted. The chamber has a platform

swivel that allows you to record outside the marked location. The owner also

dedicated to PUBLISHING the images/videos you capture with the camera in groups of

WhatsApp. He also uses it to spy on the private conversations of employees.

and customers who come to the bar.

Next I will attach an image that the owner of the establishment has

Shared in a Whatsapp group. The image is dated by the

video camera. In it you can see the outside of the premises, the center corridor

where the rest of the people who come to the center to go to other

local.

As I mentioned earlier, the camera is rotatable so you usually control it

and change your position daily. It can also be seen at the bottom as the

sound icon is active, so you are listening to conversations on

that very moment."

It provides images of the location of the cameras.

SECOND: Prior to the acceptance of this claim for processing, it is

transferred to the claimed party, in accordance with the provisions of article 65.4 the

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

of digital rights (hereinafter, LOPDGDD), being received on the date

October 14, 2021, as stated in the proof of delivery issued by the service of

emails.

Given the lack of response, said transfer was reiterated, being returned by the

emails with the annotation "Unknown".

THIRD: The claim was admitted for processing by means of a resolution of 20

December 2021.

FOURTH: On March 2, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimed party, for

the alleged infringement of articles 5.1.c) and 13 of the RGPD, typified in article

83.5 of the GDPR.

FIFTH: On March 18, 2022, the notification of the

Agreement to Start the Sanctioning Procedure with the annotation “Returned to Origin by surplus (Not withdrawn in the office)”.

On March 31, said shipment was reiterated, being returned again with the annotation “Returned to origin by unknown”.

Therefore, it was sent to the Single Edictal Board (TEU), being published on the 27th of April 2022.

There is no record that, at the present time, the respondent has submitted a written allegations to it.

Article 64.2.f) of Law 39/2015, of October 1, on Administrative Procedure Common Public Administrations (hereinafter LPACAP) -provision of which the party claimed was informed in the agreement to open the proceeding- establishes that if allegations are not made within the stipulated period on the content of the agreement of initiation, when it contains a precise pronouncement about the imputed responsibility, may be considered a resolution proposal. In the present case, the agreement to initiate the disciplinary proceedings determined the facts in which the imputation was specified, the infraction of the RGPD attributed to the claimed and the penalty that could be imposed. Therefore, taking into consideration that the part claimed has not made allegations to the agreement to initiate the file and in attention to what is established in article 64.2.f) of the LPACAP, the aforementioned initial agreement is considered in this case proposed resolution.

In view of everything that has been done, by the Spanish Data Protection Agency In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: On September 20, 2021, it entered this Agency claim of D.A.A.A. against the defendant for having installed a security camera video surveillance with a rotating platform that allows you to record outside the premises

Cafeteria

STREET

***DIRECTION.1 and that captures audio, also lacking informative signs.

*** SHOPPING CENTER.1,

***CAFETERIA.1

DC

of

SECOND: Photographs of the location of the camera are provided.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/11

FOUNDATIONS OF LAW

Yo

In accordance with the powers that article 58.2 of the RGPD grants to each authority of control and according to what is established in articles 47 and 48.1 of the LOPDGDD, it is competent to initiate and resolve this procedure the Director of the Agency Spanish Data Protection.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures processed by the Spanish Agency for Data Protection will be governed by the provisions in Regulation (EU) 2016/679, in this organic law, by the provisions regulations issued in its development and, as long as they do not contradict them, with a subsidiary, by the general rules on administrative procedures.”

II

The physical image of a person under article 4.1 of the RGPD is personal data

and its protection, therefore, is the subject of said Regulation. Article 4.2 of the GDPR defines the concept of “treatment” of personal data.

Article 22 of the LOPDGDD establishes the specificities of data processing for video surveillance purposes, indicating the following:

"1. Natural or legal persons, public or private, may carry out the processing of images through camera systems or video cameras with the purpose of preserving the safety of people and property, as well as their installations.

2. Images of public roads may only be captured to the extent that it is essential for the purpose mentioned in the previous section.

However, it will be possible to capture the public road in an extension superior when necessary to guarantee the security of goods or installations strategic or infrastructure linked to transport, without in any case may involve capturing images of the interior of a private home.

3. The data will be deleted within a maximum period of one month from its collection, except when they had to be kept to prove the commission of acts that threaten the integrity of persons, property or facilities. In that case, The images must be made available to the competent authority within a period maximum of seventy-two hours from the knowledge of the existence of the recording.

The blocking obligation provided for in article 32 of this organic law.

4. The duty of information provided for in article 12 of the Regulation (EU) 2016/679 will be understood to be fulfilled by placing an informative device in a sufficiently visible place identifying, at least, the existence of the treatment, the

identity of the person in charge and the possibility of exercising the rights foreseen in the Articles 15 to 22 of Regulation (EU) 2016/679. It may also be included in the informative device a connection code or internet address to this information.

In any case, the data controller must keep available to those affected the information referred to in the aforementioned regulation.

5. Under article 2.2.c) of Regulation (EU) 2016/679, it is considered excluded from its scope of application the treatment by a natural person of images that they only capture the interior of their own home.

This exclusion does not cover processing carried out by a security entity private that had been contracted for the surveillance of a home and had access to the images.

6. The processing of personal data from images and sounds obtained through the use of cameras and video cameras by the Forces and Security Bodies and by the competent bodies for surveillance and control in the penitentiary centers and for the control, regulation, surveillance and discipline of traffic, shall be governed by the legislation transposing Directive (EU) 2016/680, when the processing is for the prevention, investigation, detection or prosecution of criminal offenses or execution of criminal sanctions, including protection and prevention against threats to public safety. out of these assumptions, said treatment will be governed by its specific legislation and additionally by Regulation (EU) 2016/679 and this organic law.

7. What is regulated in this article is understood without prejudice to the provisions of

Law 5/2014, of April 4, on Private Security and its development provisions.

8. The treatment by the employer of data obtained through information systems

cameras or video cameras is subject to the provisions of article 89 of this law

organic."

III

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

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

following requirements:

- Respect the principle of proportionality.

- When the system is connected to an alarm center, you can only

be installed by a private security company that meets the requirements

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

- The video cameras will not be able to capture images of the people who

are outside the private space where the security system is installed.

video surveillance, since the processing of images in public places can only be

carried out, unless there is government authorization, by the Forces and Corps of

Security. Nor can spaces owned by third parties be captured or recorded without the

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

find.

This rule admits some exceptions since, on some occasions, for the protection of

private spaces, where cameras have been installed on facades or inside,

it may be necessary to guarantee the security purpose the recording of a portion of public road. That is, cameras and video cameras installed for the purpose of security will not be able to obtain images of public roads unless it is essential for said purpose, or it is impossible to avoid it due to the location of those and, extraordinarily, the minimum space for said purpose. Therefore, the cameras could exceptionally capture the portion minimally necessary for the intended security purpose.

- The duty to inform those affected provided for in articles 12 and 13 of the RGPD, and 22 of the LOPDGDD, in the terms already indicated.
- The person in charge must keep a record of treatment activities carried out under its responsibility, including the information to which it makes reference article 30.1 of the RGPD.
- The installed cameras cannot obtain images from private space of third party and/or public space without duly accredited justified cause, nor can affect the privacy of passers-by who move freely through the area. No this allowed, therefore, the placement of cameras towards the private property of neighbors with the purpose of intimidating them or affecting their private sphere without just cause.
- In no case will the use of surveillance practices be admitted beyond the environment object of the installation and in particular, not being able to affect the spaces surrounding public, adjoining buildings and vehicles other than those accessing the guarded space.

In summary and to facilitate the consultation of interested parties, the Spanish Agency for Data Protection offers through its website [https://www.aepd.es] access to the legislation on the protection of personal data, including the RGPD and the LOPDGDD (section “Reports and resolutions” / “regulations”), as well as the Guide on the use of video cameras for security and other purposes, as well as the Guide for the

compliance with the duty to inform (both available in the section “Guides and

tools").

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

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

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

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

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

guideline security considered minimum.

IV

On the other hand, it must be remembered that the voice is personal data because it is

of a peculiar and individual characteristic of each person that makes it identifiable, and

that the recording or amplification of the sound of voice constitutes data processing

personal.

In this case, the system installed by the claimed party also allows the capture

of the sound being able to access, as the claimant party affirms, the “conversations

employees and customers who come to the bar"

The fact that compliance with the requirements set forth in article 22 of the

LOPDGDD can legitimize video surveillance for security reasons does not imply

necessarily that the recording of the voice be legitimized, treatment that will have to have

its own justification, which does not happen in this case.

The use of the questioned system that allows the listening or recording of the

conversations of both employees and customers, to the extent that the system will allow to capture private conversations may be disproportionate and incompatible with the principle of minimization since it supposes an excessive interference in the right to privacy, as can be deduced from STC 98/2000, which in this regard points out: “the implementation of the audition and recording system has not been in this case in accordance with the principles of proportionality and minimum intervention that govern the Modulation of fundamental rights by the requirements of the interest of the business organization, since the purpose pursued (to give a plus of security, especially in the event of possible customer complaints) is disproportionate to the sacrifice that implies the right to privacy of the workers (and even casino patrons). This system allows capturing private comments, both from customers and casino 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 the workers who, in any case, are going to feel constrained to make any type of personal comment before the conviction that they will be heard and recorded by the company. It is, in short, a illegitimate interference in the right to privacy enshrined in art. 18.1 CE, well no there is a definitive argument that authorizes the company to listen and record the private conversations that casino workers have with each other or with customers” (FJ 9).

In accordance with this constitutional doctrine, the LOPDGDD recognizes, in its article 89, the right to privacy against the use of video surveillance devices and sound recording in the workplace. Article 89 specifies how the employer adopt these business control measures, by providing the following:

1. Employers will be able to treat the images obtained through systems

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

workers or public employees provided, respectively, in article 20.3

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

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

same. Employers must inform in advance, and expressly,

clearly and concisely, to workers or public employees and, where appropriate, to their

representatives, about this measure.

In the event that the flagrant commission of an illegal act has been detected

by public workers or employees, it shall be understood that the duty of

report when there is at least the device referred to in article 22.4 of

this organic law.

2. In no case will the installation of video recording systems be allowed.

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

workers or public employees, such as changing rooms, toilets, dining rooms and

analogues.

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

for the recording of sounds in the workplace will be admitted only when

risks to the safety of facilities, goods and people are relevant

arising from the activity carried out in the workplace and always respecting

the principle of proportionality, the principle of minimum intervention and the guarantees provided for in

the previous sections. The suppression of sounds preserved by these systems

The recording will be carried out in accordance with the provisions of section 3 of article 22 of

is

law.

Thus, the recording of sounds in the workplace can only be done

when the risks for the security of the installations, assets and

people derived from the activity that takes place in the workplace and always

respecting the principle of proportionality, that of minimum intervention and the guarantees

that article 89 itself provides.

Therefore, in those cases in which such risks concur, the recording of the voice of the

people must be justified and proportional. To check if a measure

restrictive of a fundamental right exceeds the judgment of proportionality, it is necessary

Check if you meet the following three requirements or conditions:

1. That it is a measure capable of achieving the proposed objective (judgment of

suitability).

2. That there is no other more moderate measure to achieve such purpose with

equal efficacy (judgment of necessity).

3. That it be weighted or balanced, because it derives more benefits or

advantages for the general interest than harm to other goods or values in conflict”

(judgment of proportionality).

In this case, the respondent party has not proven the concurrent circumstances that

could justify the proportionality of the measure has not even declared its purpose,

so it can be concluded that the use of this video surveillance system that allows

capturing private comments from natural persons also violates the principle of

data minimization for this reason.

v

In the present case, the claim was filed because the respondent has installed a

video surveillance camera with a rotating platform that allows it to record outside the

local cafeteria ***CAFETERIA.1 del

***DIRECTION.1 and that captures audio, also lacking informative signs.

DC *** SHOPPING CENTER.1,

STREET

As proof of these statements, the claimant provided the evidence indicated

in the “Facts” section of this agreement.

The corrective powers available to the Spanish Agency for the Protection of

Data, as a control authority, is established in article 58.2 of the RGPD. Among

they have the power to issue a warning -article 58.2.b)-, the power

to impose an administrative fine in accordance with article 83 of the RGPD -article 58.2

i)-, or the power to order the person in charge or in charge of the treatment that the

treatment operations comply with the provisions of the RGPD, where appropriate,

in a certain way and within a specified period -article 58. 2 d)-.

According to the provisions of article 83.2 of the RGPD, the measure provided for in article 58.2

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

administrative.

SAW

In accordance with the evidence available and which has not been

distorted in the sanctioning procedure, the defendant has a camera installed

of video surveillance that could be capturing images of third parties, and also lacks

information poster of the existence of these cameras, so it is considered that

These facts violate the provisions of articles 5.1.c) and 13 of the RGPD, which

involves the commission of offenses typified in article 83.5 of the RGPD, which provides

the next:

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

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

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

Total annual global business of the previous financial year, opting for the one with the highest

amount:

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

consent under articles 5, 6, 7 and 9;

b) the rights of the interested parties according to articles 12 to 22;

[…]."

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

previous paragraph are considered very serious and prescribe after three years, in accordance with

Article 72.1 of the LOPDGDD, which establishes that:

"Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

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

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

following:

a) The processing of personal data violating the principles and guarantees

established in article 5 of Regulation (EU) 2016/679.

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

conditions of legality of the treatment established in article 6 of the Regulation (EU)

2016/679.

(…)

h) The omission of the duty to inform the affected party about the treatment of their

personal data in accordance with the provisions of articles 13 and 14 of the Regulation (EU)

2016/679 and 12 of this Organic Law. (…)»

7th

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

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

Therefore, it is appropriate to graduate the sanction to be imposed in accordance with the criteria established

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

Regarding section k) of the aforementioned article 83.2 RGPD:

In the initial assessment, the following have been considered:

- The nature of the offense by having a video surveillance system that

is oriented towards public transit areas without just cause, treating data of

identifiable natural persons (art. 83.5 a) RGPD.

- The intention or negligence of the infraction, the cameras are oriented

to the outside of your property (83.2.b) RGPD).

- The informative poster is incomplete, without indicating who is responsible for the

treatment or where the interested parties can go to exercise their rights

recognized in the GDPR.

viii

However, as already indicated in the initial agreement and in accordance with the

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

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

treatment comply with the provisions of this Regulation, when

appropriate, in a certain way and within a specified period […].”

requires the respondent to take the following steps:

- provide the images that are observed with the device in question, indicating

in a location plan the parts that correspond to your particular property.

- Prove that you proceeded to remove the camera from the current location, or to

reorientation of it towards its particular area.

- certifies having proceeded to place the informative device in the

video-monitored areas or to complete the information offered therein (you must

identify, at least, the existence of a treatment, the identity of the person in charge and the

possibility of exercising the rights provided for in said precepts), locating this

device in a sufficiently visible place, both in open and closed spaces.

- certifies that it keeps the information to which it refers available to those affected.

refers to the aforementioned RGPD.

It is warned that not meeting the requirements of this organization may be

considered as an administrative offense in accordance with the provisions of the RGPD,

typified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the

opening of a subsequent sanctioning administrative proceeding.

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

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES

FIRST: IMPOSE D. B.B.B., with NIF ***NIF.1, for an infraction of article

5.1.c) of the RGPD, typified in article 83.5 of the RGPD, a fine of €300

(three hundred euros).

SECOND: IMPOSE D. B.B.B., with NIF ***NIF.1, for a violation of article 13

of the RGPD, typified in article 83.5 of the RGPD, a fine of €300 (three hundred

euros).

THIRD: ORDER D.B.B.B., with NIF ***NIF.1, which, by virtue of article 58.2.d)

of the GDPR, within ten days, take the following measures:

- provide the images that are observed with the device in question, indicating

in a location plan the parts that correspond to your particular property.

- Prove that you proceeded to remove the camera from the current location, or to

reorientation of it towards its particular area.

- certifies having proceeded to place the informative device in the

video-monitored areas or to complete the information offered therein (you must

identify, at least, the existence of a treatment, the identity of the person in charge and the

possibility of exercising the rights provided for in said precepts), locating this

device in a sufficiently visible place, both in open and closed spaces.

- certifies that it keeps the information to which it refers available to those affected.

refers to the aforementioned RGPD.

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

FIFTH: Warn the sanctioned person that he must make the imposed sanction effective once

that this resolution is enforceable, in accordance with the provisions of article

98.1.b) of the LPACAP, within the voluntary payment period established in article 68 of the

General Collection Regulations, approved by Royal Decree 939/2005, dated 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 procedure number that appears in the

heading of this document, in restricted account number ES00 0000 0000 0000

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

banking entity CAIXABANK, S.A.. Otherwise, it will be collected

in executive period.

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

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

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

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

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

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

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

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

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

Interested parties may optionally file an appeal for reconsideration before the Director

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

day following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court,

in accordance with the provisions of article 25 and paragraph 5 of the additional provision

fourth of Law 29/1998, of July 13, regulating the Contentious Jurisdiction-

administrative, within a period of two months from the day following the notification

of this act, as provided for in article 46.1 of the aforementioned Law.

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

The firm resolution may be provisionally suspended in administrative proceedings if the

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

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

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

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

or through any of the other registers provided for in article 16.4 of the aforementioned

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

that proves the effective filing of the contentious-administrative appeal. If the

Agency was not aware of the filing of the contentious appeal-

within a period of two months from the day following the notification of the

This resolution would terminate the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency