 File No.: EXP202206481

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: On June 6, 2022 A.A.A. (hereinafter, the claiming party)

filed a claim with the Spanish Data Protection Agency.

The claim is directed against HERON CITY VALENCIA MANAGEMENT S.L. with

NIF-B83122937 (hereinafter, the claimed party).

The reasons on which the claim is based are the following: on June 6,

2022, by email that he provides along with his claim, he requested the party

claimed, after having tried to make your request in person at the

facilities of the claimed party, access to images from the system of

video surveillance located in its facilities, receiving a response that it provides, in the

that the claimed party indicates that such access is not possible, except when there is prior

complaint, being requested by the Police or authorized personnel, understanding the part

claimant that said response is not in accordance with the data protection regulations.

SECOND: On July 12, 2022, in accordance with article 65 of the

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

THIRD: On August 30, 2022, the Director of the Spanish Agency for

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

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1,

of the Common Administrative Procedure of Public Administrations (in

hereafter, LPACAP), for the alleged infringement of Article 15 of the GDPR, typified in

Article 83.5 of the GDPR.

FOURTH: Notification of the aforementioned initiation agreement in accordance with the established norms in Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations (hereinafter, LPACAP), the claimed party submitted a written of allegations in which, in summary, he stated that among his duties he did not include finds the video surveillance system and the processing of personal data personnel recruited through said system.

It also states that it is not aware that the claimant appeared at its offices or who communicated personally or by telephone their intention to exercise any right (an issue, on the other hand, that the claimant does not prove in any way), if it is true that you sent an electronic communication to the email address marketing@heroncityvalencia.com announcing that if it does not provide "access to recordings in which I am recorded in his mall" would put him in knowledge of this Agency.

In this sense, it indicates that the email address to which the interested party directed is not related to the processing of personal data or to the means of contact enabled for the exercise of the rights of the interested parties in the framework of the shopping center in question.

FIFTH: On September 21, 2022, the instructor of the procedure agreed carry out the following tests, assuming they have been reproduced for probative purposes the claim filed by A.A.A. and its documentation, the documents obtained and generated during the phase of admission to processing of the claim, and the report of

previous investigation actions that are part of the procedure

AT/02740/2022.

Likewise, it is considered reproduced for evidentiary purposes, the allegations to the

initiation of the referenced sanctioning procedure, presented by HERON CITY

VALENCIA MANAGEMENT, S.L., and the accompanying documentation.

SIXTH: On September 26, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

penalize HERON CITY VALENCIA MANAGEMENT, S.L., with NIF B83122937, for

an infringement of article 15 of the GDPR, typified in article 83.5 of the GDPR, with

a fine of €10,000 (ten thousand euros)

SEVENTH: On October 10, 2020, in response to the proposal of

resolution handed down, the defendant entity presented allegations stating that it has

contacted HERON CITY MEDITERRÁNEO, S.L., which claims to have a

contract for the provision of services with a company that manages the maintenance of the

installation of the CCTV (closed circuit television) equipment of the Center

Commercial of Heron City of Paterna.

By virtue of said contract, both HERON CITY MEDITERRÁNEO, S.L. -as

responsible for the treatment of the data obtained from the activity of video surveillance-

as the contracted company -as the person in charge of the treatment- are the only

entities with access to the personal data object of this file.

Despite the fact that both entities, HERON CITY VALENCIA MANAGEMENT, S.L., and

HERON CITY MEDITERRÁNEO, S.L., belong to the same business group, the

The requested entity states that it is not empowered to contribute to this procedure

copy of said contract.

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

in the file, the following have been accredited:

PROVEN FACTS

FIRST: On June 6, 2022, the claimant requests access to the images

from the video surveillance system located in its facilities, and the part

claimed

email from

marketing@heroncityvalencia.com as follows:

answers

his

you

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/11

"We indicate that the images from the video surveillance cameras can only be

required by authorized personnel or the police, and only in the event that there is a

prior complaint, so we recommend that you file the complaint.

However, we indicate that the cameras are not continuously recording, they record

for periods of time.

In case the police ask us, we would need to know the date, exact location

and time slot as close as possible to is if there is a recording in that

period.

We also indicate that the recordings self-destruct after 15 days if there is no

no police request."

SECOND. As a consequence of the foregoing, this Agency considers that it was not

respecting the right of access of the complaining party to their personal data,

as established in article 15 of the GDPR.

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: "The 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

The physical image of a person, according to article 4.1 of the GDPR, is data

personnel and their protection, therefore, is the subject of said Regulation. In article 4.2

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

The images generated by a system of cameras or camcorders are data of

personal nature, so its treatment is subject to the protection regulations

of data.

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

natural persons) carried out through the denounced video surveillance system is

in accordance with the provisions of the GDPR.

II

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

processing of personal data.

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.

Article 15 of the GDPR, recognizes the right of access stating the following:

"1. The interested party shall have the right to obtain confirmation from the data controller

whether or not personal data concerning you is being processed and, if so,

right of access to personal data and the following information:

a) the purposes of the treatment;

b) the categories of personal data concerned;

c) the recipients or categories of recipients to whom they were communicated or will be

communicated personal data, in particular recipients in third parties or organizations

international tions;

d) if possible, the expected period of conservation of personal data or, if not

if possible, the criteria used to determine this term;

e) the existence of the right to request from the person in charge the rectification or deletion of

personal data or the limitation of the processing of personal data relating to the interest

data, or to oppose said treatment;

f) the right to file a claim with a control authority;

g) when the personal data has not been obtained from the interested party, any information

mation available on its origin;

h) the existence of automated decisions, including profiling, to which

referred to in Article 22, paragraphs 1 and 4, and, at least in such cases, significant information

information about the logic applied, as well as the importance and the consequences foreseen

of said treatment for the interested party.

2. When personal data is transferred to a third country or to an international organization

national, the interested party shall have the right to be informed of the appropriate guarantees in

under article 46 relating to the transfer.

3. The data controller shall provide a copy of the personal data object of

treatment. The person in charge may receive for any other copy requested by the

terested a reasonable fee based on administrative costs. When the interest

application is submitted by electronic means, and unless the latter requests that it be

otherwise provided, the information will be provided in a commonly used electronic format.

bad

4. The right to obtain a copy mentioned in section 3 will not negatively affect

to the rights and liberties of others."

IV.

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

video surveillance, to comply with current regulations, must comply with the

following requirements:

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

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

as well as its facilities.

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

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

should be processed if the purpose of the processing cannot reasonably be achieved by

other means, recital 39 of the GDPR.

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

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

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

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

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

a “layered information” system.

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

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

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

processing of personal data.

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

visible and must be provided in advance.

Second layer information should be easily available in one place

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

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

other elements of article 13 of the GDPR.

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

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

It can be carried out by the Security Forces and 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

RGPD and the LOPDGDD (section "Reports and resolutions" / "regulations"),

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

the Guide for compliance with the duty to inform (both available at the

section "Guides and tools").

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

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

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

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

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

indicative security considered minimum.

V

In the present case, the right of access to the claimant is denied, stating that he

lack of competence or treatment of such data as expressed in the

allegations forwarded to this Agency, but it indicates to the claimant that they will be

denies access to them because according to the claimed entity they only have

right of access to recordings by authorized personnel or the police.

It follows from these statements that the respondent entity acknowledges that it leads to

carry out recordings and therefore is responsible for the processing of personal data, in

of the image, and that in this case the right of access to the

claimant.

Throughout the proceedings, the claimed entity claims not to be the responsible entity,

and affirms that he cannot provide the document that confirms it despite stating that the

responsible is another entity of the same business group.

In this sense, note that those in charge of treatment have the obligation to

assist the controller, taking into account the nature of the processing, through

appropriate technical and organizational measures, whenever possible, so that this

can comply with its obligation to respond to requests that have the purpose of

the exercise of the rights of the interested parties established in chapter III, according to

provides for article 28.3.e) of the GDPR. This obligation is incumbent on all managers

whether or not they are part of the manager's business group and the contract must

stipulate how the processor will provide that assistance to the controller.

In this case we do not know what type of assistance has been agreed or even the

claimed certifies that he acts as the person in charge of the treatment and even in the case of

act as data processor, the claimed entity should have at least transferred

the request for access to the person in charge, since the evaluation of whether the requests of the

Interested parties are admissible or if the requirements established by the GDPR are met

must be carried out by the data controller, as stated in the Guidelines

07/2020 on the concepts of controller and processor in the GDPR. Version 2.0.

adopted on July 07, 2021.

Thus, even if the claimed entity were in charge, it would be responsible for the

infringement since it made the decision not to provide the claimant with access to the recording

instead of transferring it to the person in charge

Therefore, it is considered that the facts exposed, that is, not giving access to the

claimant to the recordings that were made about him and his vehicle in the

facilities of the defendant, and not being able to prove their lack of responsibility,

considers that article 15 of the GDPR has been violated, which implies the commission of

an infringement typified in article 83.5 of the GDPR, which provides the following:

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

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

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

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

of greater 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,

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

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

following:

(…)

k) The impediment or the obstruction or the reiterated non-attention of the exercise of the

rights established in articles 15 to 22 of Regulation (EU) 2016/679."

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.

SAW

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Therefore, it is appropriate to graduate the sanction to be imposed according to the criteria that

establishes article 83.2 of the GDPR, and with the provisions of article 76 of the

LOPDGDD, with respect to section k) of the aforementioned article 83.2 GDPR.

Article 83.2 of the GDPR establishes that:

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

individual case, as an addition to or substitute for the measures contemplated in article

Article 58, section 2, letters a) to h) and j).

When deciding to impose an administrative fine and its amount in each individual case

dual will be duly taken into account:

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

nature, scope or purpose of the processing operation in question

such as the number of interested parties affected and the level of damages that

have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to

alleviate the damages and losses suffered by the interested parties;

d) the degree of responsibility of the controller or processor,

taking into account the technical or organizational measures that they have applied under

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 whether the person in charge or the person in charge notified the infringement and, if so, in 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 to mechanisms of

certification approved in accordance with 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 infringement."

In the present case, the clear intentionality of

of the entity claimed for the commission of the acts object of this procedure

sanction, according to article 83.2 b) of the GDPR, since access is not allowed by

part of the claimed entity, to the recording images of the image of the

complainant and his vehicle, nor indicate to whom he could exercise such

rights, in the event that such services were entrusted to another company

belonging to the same business group, as it has indicated in its allegations.

For all these reasons, it is considered that the sanction that would correspond to be imposed would be 10,000

euro.

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 HERON CITY VALENCIA MANAGEMENT, S.L., with NIF

B83122937, for a violation of article 15 of the GDPR, typified in article 83.5

of the GDPR, a fine of 10,000 euros (ten thousand euros).

SECOND: NOTIFY this resolution to HERON CITY VALENCIA

MANAGEMENT, S.L.

THIRD: Warn the penalized person that they must make the imposed sanction effective

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

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

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

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

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

of December 17, by means of its income, indicating the NIF of the sanctioned and the number

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

restricted number ES00 0000 0000 0000 0000 0000, open in the name of the Agency

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

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

Once the notification has been received and once executed, if the execution date is

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

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

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

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

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

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

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

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

Interested parties may optionally file an appeal for reversal before the

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

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

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

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

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

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

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

referred Law.

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

may provisionally suspend the firm resolution in administrative proceedings if the

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

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

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

of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other registries provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative proceedings within a period of two months from the day following the Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency