938-0419

Procedure No.: PS/00390/2018

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On May 29, 2018, the claim is registered

formulated by Ms. AAA, (hereinafter, the claimant), stating that

one of the cameras of the video surveillance system installed by the entity COFEMEL

SOCIEDADE DE VESTUARIO S.A., BRANCH IN SPAIN, (hereinafter, the

claimed), in the establishment with trade name TIFFOSI, located in the Center

Comercial LA GAVIA of ***ADDRESS.1, is located in the staff locker room

and rest area, assuming data processing that seriously violates the

employees' right to privacy.

According to the claimant, the images recorded by said system of

video surveillance are viewed by the supervisors of the establishment and by other

middle management, as is the case with the store manager, who also

you can view them remotely from your own home.

Similarly, the claimant alleges that the system monitor is located in the

aforementioned changing room, a dependency that also serves as a warehouse, for which the

Captured images are visible to all employees. It also adds that the

Informative video surveillance zone sign is not clearly visible when placed

at ground level.

The claimant attaches two photographs. One of which, according to the complainant,

corresponds to the camera located in the locker room and shows some lockers that

They have clothes hanging. The other photo shows part of a keyboard and a monitor.

SAMSUNG showing nine images dated May 16, 2018

from different areas of the commercial establishment in question.

SECOND: Dated September 11, 2018, it has an entry in this Agency

written document from the legal representative of the claimed party to whom, in response to the request

of information formulated to said Company, the following documentation is attached:

-

Printing of the informative poster of the video-monitored area, in which

identifies the claimed person as responsible for the video surveillance treatment. East

The poster does not offer all the information that must be provided to the interested parties, nor does it offer a

layered information system that enables access to it. Among other

irregularities, it is observed that the data protection rights that

can be exercised before the data controller taking into account the

specialty of the matter of video surveillance (rights of access, deletion and

limitation of treatment recognized in articles 15, 17 and 18 of the RGPD).

-

A photograph of the aforementioned poster which, according to the respondent, was

displayed in the front of the store, although the photograph provided does not allow us to know the

exact location of the poster by not showing the exact place of its placement, so

does not prove that it is placed, in a visible way, at the entrances to the area

guarded

-

An indicative map of the nine cameras installed in the store. The

document provided is not dated nor does it allow to identify the location and nomenclature

of each of the devices as the written information contained is not legible

in the same.

-

Copy of the viewing panel of the cameras, where, as indicated

by the defendant, you can see the areas recorded on August 27,

2018 and that do not record images of adjoining land and houses or foreign space.

The response made does not provide any information regarding the existence

of the video surveillance camera photographed by the claimant and located, according to her,

in an area used as a locker room and warehouse, and about which nothing is reported by the

claimed, not allowing to associate said camera with any of the images of the

panel photographed or with its location on the plan or with the purposes for which it was

use the area video-surveillated by that camera.

The respondent has not provided information that justifies the exact place where

which have been and/or are the monitor and recorder, persons authorized for the

viewing of the images, security measures adopted to protect the

confidentiality and restrict access to images, confirmation of whether it can be

access them remotely as indicated by the claimant.

THIRD: Accessed on January 11, 2018, the application of the AEPD that manages

the consultation of the history of sanctions and previous warnings, is verified

that the claimed party does not have previous records.

FOURTH: On January 18, 2019, the Director of the Spanish Agency for

Data Protection agreed, in accordance with the provisions of article 58.2 of the

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27,

2016, regarding the protection of natural persons with regard to the treatment

of personal data and the free circulation of these data, (hereinafter RGPD),

start sanctioning procedure against COFEMEL SOCIEDADE DE VESTUARIO S.A.,

BRANCH IN SPAIN, for the alleged infringement of both sections c) and f) of the

article 5 of the RGPD and article 13 of the same Regulation, typified,

respectively, in article 83.5.a) and b) of the RGPD, considering that the sanction that

could correspond would be a WARNING, without prejudice to what would result from

The instruction.

FIFTH: On February 7, 2019, a written entry of

allegations of the legal representative of the defendant in which, in summary, it is indicated:

-

In relation to the video camera located in the warehouse of the store,

points out that, as can be verified in the documentation provided previously,

the angle of it was reduced in order to limit the recording to the back door and

computer, in such a way that it did not capture images of the rest area/changing room

staff, as evidenced by the smaller size of the screen that shows the

images collected by camera 9, corresponding to the warehouse. They indicate that

Attached documentation that shows the image of the security cameras and the zoom

-

to show that no images are recorded in the area corresponding to the

rest / locker room of employees.

Technical and organizational measures have been taken to ensure that

access to the visualization of the captured images is limited, only in case

of necessity, to two employees of the IT department, whose identification is provided,

that must be within the network/VPN, know the access IP and identify themselves with

user and password. These same employees are also authorized to view

said images via remote

Images are kept for 30 days and are automatically deleted.

The list of rights has been included in the notice poster,

making available to interested parties an additional informative document that

extensive and detailed information. Photographs are attached showing the places where

that the video-surveillance area sign has been placed (escape, warehouse and box),

printing of the content of the informative poster and document with the information

complementary to it.

-

-

SIXTH: In view of everything that has been done, by the Spanish Protection Agency

of Data in this procedure the following are considered proven facts,

FACTS

First: On May 29, 2018, you have entered this Agency in writing from the

claimant stating that the supervisors and middle managers of the

“TIFFOSI” brand store in the “La Gavia” Shopping Center in Madrid

access indiscriminately, and even remotely in the case of the person in charge, to

the recordings of the images captured by the video surveillance cameras

installed in said commercial premises by the entity COFEMEL SOCIEDADE DE

VESTUARIO S.A., SUCURSAL EN ESPAÑA, (the defendant), having, therefore,

access to the images collected by the camera located in the locker room and

rest of the store staff, thereby violating the right to privacy of

the workers of said premises.

The claimant adds that the monitor that shows the images collected by

the different cameras of the video surveillance system is visible to all

employees who access said locker room, also used as a warehouse.

At the same time, the claimant points out that the information sign for the zone

video surveillance is not clearly visible as it is placed at ground level.

Second: The claimant attaches to her claim two photographs taken in the area

locker room of the reviewed business premises. In the photograph that, according to the claimant,

shows the “Image of the video recording camera installed in the changing rooms of the

staff”, a camera installed in an area with several lockers with clothing is observed.

hanging.

In the other photograph, which, according to the claimant, shows the “Image of the monitor

of the cameras, captured by being installed in full view of all”, appears part of a

keyboard and a SAMSUNG monitor displaying nine images dated the

May 16, 2018 from different areas of the business premises in question, in one of the

which featured a microwave and refrigerator.

Third: The claimed party is responsible for the processing of personal data derived

of the installation in the aforementioned store of an integrated video surveillance system

by nine chambers, one of which, identified as chamber 9, is located in

an outbuilding used as a dressing room and rest area by employees, which

It is also used as a warehouse. The images obtained can be viewed in

real time and remotely. These images are recorded, conserving

stored for 30 days and automatically deleted.

Fourth: On September 11, 2018, the respondent presents, among other things, the

following documentation:

4.1. printing of the informative poster of "Video Surveillance Zone", including:

identification of the claimed person as responsible for the video surveillance treatment and address of the same; form and means through which to exercise the rights of data protection before the same, legitimizing basis of the treatment and purposes of the same.

4.2. Printout of nine images that, according to the respondent, were obtained on August 27, 2018 from the viewing panel of the cameras of the video surveillance system of the commercial premises.

Fifth: On February 7, 2019, the respondent has alleged the implementation of the following technical and organizational measures:

5.1 Reducing the angle of the camcorder 9 so as not to capture images of rest area/staff locker room. Attach printout of image capture obtained from camera 9 dated January 30, 2019 showing a door and computer equipment.

5.2 Restricted access to viewing the images captured by the video surveillance system, including remote access, to two authorized persons that must be within the network/VPN, know the access IP and identify themselves with user and password.

5.3 Modification of the informative poster of “Video Surveillance Zone”, including detail of the rights provided for in articles 15, 17 and 18 of the RGPD and a mechanism to obtain more information, consisting of making available to the interested parties a document containing the remaining additional information on the aspects included in article 13 of the RGPD. Attached print of the poster of "Zona CCTV” and the document with the additional information made available to the interested.

5.4 Placement of said poster in the shop window, warehouse and box of the premises.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that articles 55.1, 56.2 and 58.2 of the Regulation

(EU) 2016/679 of the European Parliament and of the Council of 04/27/2016 regarding the

protection of natural persons with regard to data processing

personal information and the free circulation of these data, (hereinafter, RGPD), recognizes

each control authority, and as established in articles 47 and 48.1 of the Law

Organic 3/2018, of 5/12, on the Protection of Personal Data and guarantee of the

digital rights, (hereinafter LOPDGDD), the director of the AEPD is competent

to start and to resolve this procedure.

Article 63.2 of the LOPDGDD establishes 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

Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the

Council of April 27, 2016, regarding the protection of natural persons in relation to

regarding the processing of personal data and the free circulation of these data

(General Data Protection Regulation, hereinafter RGPD), under the rubric

“Definitions”, provides that:

“For the purposes of this Regulation, the following shall be understood as:

1) "personal data": any information about an identified natural person or

identifiable ("the interested party"); An identifiable natural person shall be deemed to be any person

whose identity can be determined, directly or indirectly, in particular by

an identifier, such as a name, an identification number,

location, an online identifier or one or more elements of the identity

physical, physiological, genetic, psychic, economic, cultural or social of said person;

2) "processing": any operation or set of operations carried out

about personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structuring,

conservation, adaptation or modification, extraction, consultation, use,

communication by transmission, broadcast or any other form of enabling of

access, collation or interconnection, limitation, suppression or destruction;”

Therefore, in accordance with these definitions, the capture of images

natural persons, identified or identifiable,

through systems of

video surveillance, constitutes a treatment of personal data, regarding the

which the data controller must comply with the provisions of article

13 of the GDPR.

III

In the first place, the defendant, in his capacity as responsible for the

treatment for video surveillance purposes carried out in the indicated commercial premises, a

infringement of the provisions of sections c) and f) of article 5 of the RGPD, which

determine in terms of the "Principles relating to treatment" that:

“Personal data will be:

(…)

c) adequate, relevant and limited to what is necessary in relation to the purposes

for which they are processed (“data minimization”).

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized or unlawful processing and

against its loss, destruction or accidental damage, through the application of measures

appropriate technical or organizational (“integrity and confidentiality”)”

At the same time, article 5 of the LOPDGDD, under the heading "Duty to

confidentiality”, states that:

"1. Those responsible and in charge of data processing as well as all

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary

of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain

even when the relationship of the obligor with the person in charge or person in charge had ended

of the treatment”.

These precepts must be related to the provisions of article 22.1 and 8 of

the LOPDGDD for cases of "Processing for video surveillance purposes",

provided therein that:

"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 persons and goods, as well as their

installations.

(…)

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.”

Article 89 of the LOPDGDD, under the heading "Right to privacy against the

use of video surveillance and sound recording devices in the workplace

work", in its section 2 provides the following:

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

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

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

analogues.

IV

Article 5.1.c) of the RGPD includes as one of the principles related to the

treatment of data minimization, according to which the data object of

treatment in the field of video surveillance must be adequate, pertinent and

limited in relation to the security purposes for which they are processed, and must

Limit the processing of images to the minimum necessary or essential for the

intended purpose.

So not only the number of cameras should be limited to the necessary

to fulfill the surveillance function, but also the monitors and the

recording should be located in guarded places or restricted areas, so that, in

As far as possible, they are not exposed to the public. In addition, the images

should only be accessible to personnel authorized to control the

display and recording devices. At the same time, if the access is done with

Internet connection will be restricted with a user code and password, or

any other means that guarantees unequivocal identification and authentication, which only

They will be known by the people authorized to access said images.

In this case, through the graphic documentation provided by the

claimant described in the Second Proven Fact and as can be deduced from the

own allegations made by the respondent when communicating the measures adopted
to regularize the situation, it has been proven that on the date of the claim the
video surveillance image display monitor and video recording system
they were located in the locker room and rest area, in such a way that the
images displayed through those devices were not displayed in one place
guarded or restricted access.
The claimant also reported the indiscriminate access to the images
recorded by the supervisors and middle managers of the store in real time and in
remotely by the manager. Regarding this access by unauthorized personnel,
the respondent has alleged that the viewing of the images has been restricted
captured by the video surveillance system, including remote access, to two
authorized persons who must be within the network/VPN, know the access IP
and identify with username and password, although it does not justify the location of the monitor
and the recording system in a guarded place or with restricted access or the causes
that limit or prevent said measure.
In addition, it is accredited in the procedure that camera number 9 has come
collecting images in a room that is used as a dressing room and
break by store staff, a circumstance that inevitably affects the
right to privacy and to the image of the employees who have used said
space for those specific purposes that affect your privacy. this treatment
However, it has occurred that, by virtue of the principle of data minimization, the
claimed must assess the possibility of adopting other less intrusive means to the
privacy of individuals to prevent unjustified interference with the rights and
fundamental liberties.
In relation to this particular, it should not be ignored that Organic Law 1/1982,
of May 5, Civil Protection of the Right to Honor, Personal Privacy and

Family and Own Image, provides in its article 7 that:

“They will be considered illegitimate interference in the field of

protection determined by the second article of this Law:

1. The placement in any place of listening devices, filming,

of optical devices or any other means suitable for recording or reproducing life

intimate of people.

2. The use of listening devices, optical devices, or any other

other means for the knowledge of the intimate life of people or

statements or private letters not addressed to those who make use of such means,

as well as its recording, registration or reproduction.”

The fact that video surveillance may be legitimate for reasons of

safety of facilities, people and goods, does not necessarily imply that the

collection and recording of images in certain spaces whose use affects the

personal privacy is legitimate and proportionate. Consequently, the

installation of a video surveillance camera in changing rooms, bathrooms and

rest spaces for workers does not comply with the principle of minimization of

data, estimating an intrusive measure for the privacy of the workers of the premises

and the protection of your right to personal data.

After receiving the agreement to initiate the procedure, the

claimed has indicated that the angle of video camera No. 9 has been reduced so as not to

capture images of the rest area and staff locker room, providing

impression of image capture obtained on January 30, 2019 from that

device in which only a door and computer equipment are captured.

However, as video surveillance cameras cannot be installed in any case

in spaces used by those affected by the treatment as changing rooms and/or areas

break it is estimated that the response offered by the respondent is insufficient

and inadequate, since this specific treatment supposes a disproportionate measure

regarding the purpose of surveillance and security pursued, and the

principle of minimization of data in certain spaces in which priority is given to

right to privacy of those affected versus the right to security.

v

With regard to the infringement of article 5.1.f) of the RGPD that includes as

One of the principles related to the treatment is that of confidentiality, in view of what

acted, it is estimated that the respondent did not adopt the technical and organizational measures

necessary tending to guarantee the security of the personal data captured by

the cameras of the surveillance system installed in the commercial premises of your brand.

The implementation of these measures would have prevented people who did not

had authorization to do so accessed, without limitation and without justification

any, to the images obtained and recorded through the video surveillance system

installed in the commercial premises, and, more particularly, they will visualize the images

collected by camera No. 9 in the unit used as a changing room and

staff break.

This uncontrolled display of images by unauthorized third parties has been

been producing at least until the respondent adopted, after the

receipt of the agreement to initiate the procedure, the technical measures and

organizational measures outlined in point 5.2 of the Fifth Proven Fact in order to limit the

access to the images obtained.

SAW

In accordance with the arguments set out in the Foundations of

Law IV and V above, COFEMEL has violated the principles of "minimization of

data" and "confidentiality" collected in sections 5.1.c) and f) of the RGPD in

in relation to the provisions of article 5 of the LOPDGDD, offense typified in the

article 83.5.a) of the RGPD and classified as very serious for the purposes of prescription in the

Article 72.1.a) of the LOPDGDD.

7th

Secondly, the defendant is charged with the violation of the provisions of the

article 13 of the RGPD, provision that regarding the "Information that must be provided

when the personal data is obtained from the interested party" determines that:

1. When personal data relating to him is obtained from an interested party, the

responsible for the treatment, at the time these are obtained, will provide

all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their

representative;

b) the contact details of the data protection delegate, if any;

c) the purposes of the treatment to which the personal data is destined and the basis

legal treatment;

d) when the treatment is based on article 6, paragraph 1, letter f), the

legitimate interests of the person in charge or of a third party;

e) the recipients or categories of recipients of the personal data,

in your case;

f) where appropriate, the intention of the controller to transfer personal data to a

third country or international organization and the existence or absence of a decision to

adequacy of the Commission, or, in the case of transfers indicated in the

Articles 46 or 47 or Article 49, paragraph 1, second paragraph, reference to the
adequate or appropriate warranties and the means to obtain a copy of these or
to the fact that they have been borrowed.

2. In addition to the information mentioned in section 1, the person responsible for the
treatment will facilitate the interested party, at the moment in which the data is obtained
personal, the following information necessary to guarantee data processing
fair and transparent

a) the period during which the personal data will be kept or, when not
possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access
to the personal data related to the interested party, and its rectification or deletion, or the
limitation of its treatment, or to oppose the treatment, as well as the right to
data portability;

c) when the treatment is based on article 6, paragraph 1, letter a), or the
Article 9, paragraph 2, letter a), the existence of the right to withdraw consent in
any time, without affecting the legality of the treatment based on the
consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or
a necessary requirement to sign a contract, and if the interested party is obliged to
provide personal data and is informed of the possible consequences of
not provide such data;

f) the existence of automated decisions, including profiling, to
referred to in article 22, sections 1 and 4, and, at least in such cases, information
about applied logic, as well as the importance and consequences
provisions of said treatment for the interested party.

3. When the person in charge of the treatment projects the subsequent treatment of

personal data for a purpose other than that for which it was collected,

will provide the interested party, prior to said further treatment, information

for that other purpose and any additional information relevant to the meaning of paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in

to the extent that the interested party already has the information.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

For its part, article 12.1 of the RGPD, referring to the “Transparency of the

information, communication and modalities of exercising the rights of the interested party”,

sets the following:

"1. The person responsible for the treatment will take the appropriate measures to facilitate

to the interested party all the information indicated in articles 13 and 14, as well as any

communication pursuant to articles 15 to 22 and 34 relating to processing, in the form

concise, transparent, intelligible and easily accessible, with clear and simple language,

in particular any information directed specifically at a child. Information

shall be provided in writing or by other means, including, if applicable, by

When requested by the interested party, the information may be provided

verbally provided that the identity of the interested party is proven by other means.”

Given the peculiarities of the treatment under study, the aforementioned

precepts must be related to the provisions of article 22.4 of the LOPDGDD for

cases of "Processing for video surveillance purposes", providing in the same

that:

"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 provided for 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.

In accordance with the aforementioned precepts, which determine the information that must be

be provided to the interested party at the time of collecting their data, and the provisions of

the aforementioned article 22.4 of the LOPDGDD, with regard to compliance with the

duty of information the person in charge of the treatment must:

1. Place at least one informative badge in the video-monitored areas

located in a visible place, and at least, at the entrances to the monitored areas, whether they are

interiors or exteriors. If there are several accesses to the video-monitored space, the aforementioned

badge must be placed on each of them.

2. The "video surveillance area" badge must inform about the existence

of the video surveillance treatment, the identity and contact details of the person responsible for the

treatment or the video surveillance system and the possibility of exercising the rights

recognized in articles 15 to 22 of the RGPD. Such information may also

be included by means of a connection code or internet address that leads to it.

Likewise, the rest of the information will be made available to the interested parties.

that must be provided to those affected in compliance with the right to information

regulated in the aforementioned Regulation (EU) 2016/679, of April 27, 2016.

In the present case, of the actions carried out, it has been proven

that prior to the initiation of this proceeding the badge or sign of

“Video Surveillance Zone” used by the claimed party or offered to the interested parties affected

viii

for this type of treatment all the information that must be provided in compliance

of the right to information regulated in article 13 of the RGPD. Specifically, the

Informative poster of "Video Surveillance Zone" presented in response to the request

of information that was made after receipt of the claim, not

specified the specific rights provided by the data protection regulations, nor

not even mentioning the most common rights in terms of video surveillance.

Likewise, it did not indicate where or how to obtain the rest of the information that must be

be provided to those affected when the personal data is obtained from the users themselves.

stakeholders, such as video surveillance images.

Likewise, it is stated in the procedure that after receiving the

initial agreement the respondent began to use the layered information system in order to

to comply with the duty to inform, facilitating in the poster of "zone

video surveillance” the basic information (first layer) and offering the information

complementary and additional (second layer) in a booklet or document made available

disposal of the interested parties in the commercial premises.

The respondent has justified said changes by providing together with his letter of

pleadings to the initiation agreement copy of the “Video Surveillance Zone” poster with the

modifications introduced in the same and of the brochure with the "Information

supplementary information on data protection”. It is observed that in said poster

including mention of the rights of access, deletion and limitation of treatment,

also introducing the reference "+info, ask our staff" in order to

make available to interested parties an additional document with the information

remaining on the aspects included in article 13 of the RGPD.

Although the "Video Surveillance Zone" poster alludes to the most

customary, a reference to the existence of other rights should be included in the

additional documentation or brochure, where you should be informed about all the

rights recognized in articles 15 to 22 of the RGPD, in accordance with the provisions of the

article 13.2.b) of the RGPD.

On the other hand, the defendant has justified the placement of the aforementioned poster in

the showcase of access to the premises and in the warehouse and next to the box.

From the foregoing, and without prejudice to the changes introduced by the person in charge

of the treatment to adapt the information offered to the aspects required in the

Article 13 of the RGPD, it is evident that COFEMEL has violated the right of

information of those affected whose personal data (images) have been subject to

treatment through video surveillance cameras installed in the business premises

of said company, which constitutes an infringement of the provisions of article 13 of the

RGPD in its relationship with the provisions of article 22.4 of the LOPDGDD, typified in

article 83.5.b) of the RGPD and qualified as minor for the purposes of prescription in the

Article 74.a) of the LOPDGDD.

Sections b), d) and i) of article 58.2 of the RGPD provide the following:

“2 Each supervisory authority shall have all of the following powers

corrections listed below:

IX

(…)

b) sanction any person responsible or in charge of the treatment with

warning when the processing operations have violated the provisions of

this Regulation;”

(...)

“d) order the person responsible or in charge of the treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate,

in a specified manner and within a specified period;”

“i) impose an administrative fine in accordance with article 83, in addition to or in

instead of the measures mentioned in this paragraph, depending on the circumstances

of each particular case;

Article 83 of the RGPD, under the heading “General conditions for the

imposition of administrative fines”, in sections 2 and 5. a) and b) states that:

"two. Administrative fines will be imposed, depending on the circumstances

of each individual case, in addition to or as a substitute for the measures contemplated

in article 58, paragraph 2, letters a) to h) and j). (…)

5. Violations of the following provisions will be sanctioned, in accordance

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

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

global total annual turnover of the previous financial year, opting for

the largest amount:

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

consent under articles 5, 6, 7 and 9;

the rights of the interested parties under articles 12 to 22;”.

b)

For its part, article 71 of the LOPDGDD establishes that "They constitute

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

this organic law.", established in articles 72.1.a) and 74.a) of said

rules the following in relation to the two offenses under study:

Regarding the violation of the principles relating to treatment, article

72.1.a) of the aforementioned Organic Law states that: "1. Depending on what is established by the

article 83.5 of Regulation (EU) 2016/679 are 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."

Regarding the violation of the duty to inform article 74 of said Law

Organic points out that: "They are considered minor and the remaining ones will expire after a year.

infractions of a merely formal nature of the articles mentioned in the

paragraphs 4 and 5 of article 83 of Regulation (EU) 2016/679 and, in particular, the

following:

a)

Failure to comply with the principle of transparency of information or the

right to information of the affected party for not providing all the information required by

Articles 13 and 14 of Regulation (EU) 2016/679."

In the present case, it is considered appropriate to impose on the defendant the sanction

of warning provided for in article 58.2.b) of the RGPD in view of the following

circumstances: it is a company whose main activity is not

linked to the usual processing of personal data, the absence of

intentionality in the offending conduct given that the treatment carried out is linked

for purposes of security of goods and people, to which is added, without prejudice to the

previously reasoned, the interest shown by the respondent in adopting with the

as quickly as possible measures aimed at correcting the irregular situation studied
and that he is not aware of the commission of any previous infringement in terms of protection
of data.
Confirmed the existence of the infractions described, and in accordance with the
established in the aforementioned article 58.2.d) of the RGPD, with regard to the infringement
of article 5.1.c) it is considered appropriate to order the data controller to
video surveillance images analyzed that technical measures are adopted and
organizational measures necessary to stop data processing operations.
video surveillance images in the locker room and rest area of the staff who
violate the principle of data minimization.
With regard to the infringement of article 13 of the RGPD, and in view of the
information currently offered by COFEMEL, it is deemed appropriate to order the
adoption of the necessary measures to include in the “Video Surveillance Zone” poster a
reference to the existence of other rights in the additional document, where
will inform about all the rights recognized in articles 15 to 22 of the RGPD,
in accordance with the provisions of article 13.2.b) of the RGPD.
It is reported that these measures must be adopted within a period of ONE
MONTH, computed from the date on which this resolution is notified
penalty, and its compliance must be proven within the same period by means of the
provision of documentation or any other means of proof valid in law that
allows verifying the cessation of the inadequate and disproportionate treatment that
It is being carried out in the previously outlined space.
It is noted that section 6 of article 83 of the RGPD, establishes that “6. The
Failure to comply with the resolutions of the supervisory authority pursuant to article 58,
paragraph 2, will be sanctioned in accordance with paragraph 2 of this article with
administrative fines of a maximum of EUR 20,000,000 or, in the case of a

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

global annual total of the previous financial year, opting for the highest amount."

Article 72.1.m) provides that: "1. According to what the article establishes

83.5 of Regulation (EU) 2016/679 are considered very serious and will prescribe to

three years the infractions that suppose a substantial violation of the articles

mentioned therein and, in particular, the following: (...)

m) Failure to comply with the resolutions issued by the authority of

competent data protection in exercise of the powers conferred by article

58.2 of Regulation (EU) 2016/679."

Therefore, in accordance with the applicable legislation and valued the

concurrent circumstances

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE COFEMEL SOCIEDADE DE VESTUARIO S.A., BRANCH

IN SPAIN, in accordance with the provisions of article 58.2.b) of the RGPD, a

sanction of WARNING for violation of the provisions of sections c) and f) of the

article 5 of the RGPD, typified in article 83.5.a) RGPD.

SECOND: IMPOSE COFEMEL SOCIEDADE DE VESTUARIO S.A., BRANCH

IN SPAIN, in accordance with the provisions of article 58.2.b) of the RGPD, a

sanction of WARNING for violation of the provisions of article 13 of the RGPD,

typified in article 83.5.b) RGPD.

THIRD: ORDER COFEMEL SOCIEDADE DE VESTUARIO S.A., BRANCH

IN SPAIN, in accordance with the provisions of article 58.2.d) of the RGPD, the

adoption and implementation of the necessary measures to:

-

To cease the processing of video surveillance images (capture,

storage and recording) that is carried out in the dependency used by the

store staff as a locker room and as a rest area, with referral from

any means of proof accrediting compliance with the requirements.

-

That the "Video Surveillance Zone" poster and the additional brochure include

the information outlined in the Basis of Law IX in relation to the

possibility of exercising the rights recognized in articles 15 to 22 of the RGPD,

in accordance with the provisions of article 13.2.b) of the same Regulation.

FOURTH: NOTIFY this resolution to COFEMEL SOCIEDADE DE

VESTUARIO S.A., BRANCH IN SPAIN, with NIF W0107301D,

In accordance with the provisions of article 50 of the LOPDPGDD, 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 art. 48.6 of the

LOPDPGDD, 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 month from

counting 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 in article 46.1 of the

aforementioned Law.

Finally, it is pointed out 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 by

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

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

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

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es