 File No.: EXP202209485

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claiming party) dated July 20, 2022

filed a claim with the Spanish Data Protection Agency. The

claim is directed against CASTILLA-LA MANCHA HEALTH SERVICE with

NIF Q4500146H (hereinafter, SESCAM). The reasons on which the claim is based are

the following:

At the beginning of 2019, SESCAM initiated a disciplinary file against the party

claimant.

On April 21, 2022, it was sent from the corporate email address ***EMAIL.1

an email to all professionals who provide services in the Management of

Urgencies, Emergencies and Sanitary Transport (G.U.E.T.S), attaching, for your

knowledge, the resolution of the disciplinary file filed against the party

claimant.

The complaining party states that the resolution sent is not found

fully anonymized; since it contains references that allow its

identification, proof of this is that he received emails from colleagues who

they had received the resolution and had identified him. In this sense, it is worth noting that

On page 5 of the resolution sent, a mention is made of the address of the

file that clearly identifies you; since, he is the only doctor of the G.U.E.T.S.

who has his residence in the Community of Canaria (knowing his colleagues

this circumstance due to its exceptionality).

Likewise, it is affirmed by the complaining party that on page 9 of said resolution

refers to the fact that on that date it was the patronal festivity in the town

where the service is provided, which allows, especially the personnel who work in the

Community of Castilla La Mancha, know perfectly well that the town in

question was Molina de Aragón, which celebrates its patron saint festivities between the 29th and 3rd

of September.

Along with the claim, provide the email sent by the claimed party to which the

attached the resolution of the disciplinary file, six emails sent

by the colleagues to the complaining party to comment on what happened and the resolution

attached to the disputed email.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of digital rights (in

LOPDGDD), the claim was transferred to SESCAM, so that

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements established in the regulations of

Data Protection.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was collected on September 15, 2022

as stated in the certificate that is in the file.

On October 18 of that same year, this Agency received a letter of

response indicating that "…To the claimant, worker of the Emergency Department and
SESCAM emergencies, a disciplinary file was opened for him for some acts of
seriousness and great repercussion in the operation and organization of the Management of
Urgencies and emergencies.
Dictated the corresponding resolution in which it proceeded to sanction said
worker, the Management withdrew all the personal data of the same in order to
send it, anonymously, to the rest of the company's workers so that they
said behaviors do not prosper and thus avoid the opening of other files
disciplinary proceedings in which other employees of the company could be harmed.
Management... Said Resolution was correctly anonymized, without the data that
appear in the Resolution that was sent, the identity of the person to whom
it means.
The name and surname of the worker did not appear in the resolution sent, nor did the center
job in which he was located, nor the geographic area in which he was located.
Neither was the person identified with initials, nor was there an address or ID. In
definitively, not only did the name of the person to whom the
Resolution, nor any other personal data that identifies the person who
had been sanctioned. There was no record of the place where he worked, nor any information that
reveal the identity of the person to whom the Resolution referred…".
THIRD: On October 20, 2022, in accordance with article 65 of the
LOPDGDD, the claim presented by the claimant party was admitted for processing.
FOURTH: On November 23, 2022, the Director of the Spanish Agency
of Data Protection agreed to initiate disciplinary proceedings against the claimed party,
for the alleged violation of article 5.1.f) of the GDPR and article 32 of the GDPR,
typified in article 83.5 of the GDPR and article 83.4 of the GDPR, respectively.
FIFTH: Notified of the aforementioned start-up agreement in accordance with the rules established in

Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP), dated December 13, 2002

was received by the Spanish Data Protection Agency in writing communicating the

intention not to make claims to the notified initiation agreement.

Article 64.2.f) of the LPACAP -provision of which the claimed party was informed

in the agreement to open the procedure - establishes that if no

arguments within the established term on the content of the initiation agreement, when

it contains a precise pronouncement about the imputed responsibility,

may be considered a resolution proposal. In the present case, the agreement of

beginning of the disciplinary file determined the facts in which the

imputation, the infringement of the GDPR attributed to the defendant and the sanction that could

impose. Therefore, taking into consideration that the claimed party has not

made allegations to the agreement to start the file and in attention to what

established in article 64.2.f) of the LPACAP, the aforementioned initiation agreement is

considered in the present case resolution proposal.

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It has been proven that on April 21, 2022, the

corporate email address ***EMAIL.1 an email to all

professionals who provide services in the Management of Emergencies, Emergencies and

Sanitary Transport (G.U.E.T.S), attaching, for your knowledge, the resolution of the

disciplinary proceedings instituted against the complaining party.

SECOND: It has been proven that the resolution sent was not found

totally anonymized, containing references that allowed the identification of the

complaining party.

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

Article 5.1.f) of the GDPR

Article 5.1.f) "Principles relating to processing" of the GDPR establishes:

"1. Personal data will be:

(…)

f) processed in such a way as to guarantee adequate security of personal data;

personal information, including protection against unauthorized or unlawful processing and against its

accidental loss, destruction or damage, through the application of technical or

appropriate organizational procedures (“integrity and confidentiality”).”

In the present case, it is clear that the personal data of the complaining party, obtained

in the SESCAM database, were improperly disseminated to the rest of the profes-

professionals who provide services in the Emergency Management, Emergencies and Transportation

Sanitary (G.U.E.T.S), violating the principle of confidentiality.

An email was sent from the corporate email address ***EMAIL.1 to

all professionals who provide services in the Emergency Department, Emergency

and Sanitary Transport (G.U.E.T.S), enclosing, for your information, the resolution

tion of the disciplinary file initiated against the complaining party.

Said resolution is not completely anonymous, containing references

that allow the identification of the complaining party.

In this sense, we must remember the definition of personal data contained in the

Article 4 of the GDPR: "... "personal data": any information about a natural person

identified or identifiable ("the data subject"); will be considered an identifiable natural person

any person whose identity can be determined, directly or indirectly, in particular

be identified by an identifier, such as a name, an identification number,

information, location data, an online identifier or one or more elements of your own

of the physical, physiological, genetic, psychological, economic, cultural or social identity of different

cha person…”.

Without forgetting that, in recital 26 of the same legal text, it is provided that the main

data protection rules should apply to all information relating to a person

identified or identifiable physical sound.

Classification of the infringement of article 5.1.f) of the GDPR

II

The aforementioned infringement of article 5.1.f) of the GDPR supposes the commission of the infringements

typified in article 83.5 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

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

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

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

overall annual total 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

lien under articles 5, 6, 7 and 9; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that:

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to

rias to the present organic law".

For the purposes of the limitation period, article 72 "Infringements considered very serious"

you see" of the LOPDGDD indicates:

"1. 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:

a) The processing of personal data in violation of the principles and guarantees established

two in article 5 of Regulation (EU) 2016/679. (…)”

Penalty for violation of article 5.1.f) of the GDPR

IV.

Article 83 "General conditions for the imposition of administrative fines" of the

GDPR section 7 establishes:

"Without prejudice to the corrective powers of the control authorities under art.

Article 58(2), each Member State may lay down rules on whether

of, and to what extent, imposing administrative fines on public authorities and bodies

public establishments established in that Member State.”

Likewise, article 77 “Regime applicable to certain categories of liability”

responsible or responsible for the treatment" of the LOPDGDD provides the following:

"1. The regime established in this article will be applicable to the treatment of

who are responsible or in charge: ...

c) The General State Administration, the Administrations of the communi-

autonomous entities and the entities that make up the Local Administration…

2. When the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this organic law

only, the data protection authority that is competent will issue a resolution

sanctioning them with warning. The resolution will also establish the

measures that should be adopted to cease the conduct or to correct the effects of the

offense that was committed.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

enough evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on the disciplinary or sanctioning regime that

be applicable.

Likewise, when the infractions are attributable to authorities and executives, and

accredit the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution in which the

sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or regional Gazette that

corresponds.

4. The data protection authority must be informed of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article. (…)”

V

GDPR Article 32

Article 32 "Security of treatment" of the GDPR establishes:

"1. Taking into account the state of the art, the application costs, and the nature of

nature, scope, context and purposes of processing, as well as probability risks

and variable severity for the rights and freedoms of natural persons, the responsibility

responsible and the person in charge of the treatment will apply appropriate technical and organizational measures.

measures to guarantee a level of security appropriate to the risk, which, where appropriate, will include

yeah, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to guarantee the confidentiality, integrity, availability and re-

permanent silence of treatment systems and services;

c) the ability to restore the availability and access to personal data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of effectiveness

technical and organizational measures to guarantee the security of processing

I lie.

2. When assessing the adequacy of the security level, particular account shall be taken of

The risks presented by the data processing, in particular as a consequence

of the destruction, loss or accidental or illegal alteration of personal data transmitted

collected, preserved or processed in another way, or the unauthorized communication or access

two to said data.

3. Adherence to a code of conduct approved under article 40 or to a mecha-

certification document approved in accordance with article 42 may serve as an element to

demonstrate compliance with the requirements established in section 1 of this

article.

4. The controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and having

ga access to personal data can only process such data following instructions

of the controller, unless it is required to do so by Union law or by

the Member States".

In the present case, at the time of the security breach, there is no record
that SESCAM had reasonable security measures based on the pos-
possible estimated risks.

SESCAM states that "The Resolution sent to all workers was revised
sada by 3 people in order to eliminate existing personal data. The Re-
solution passed 3 filters before being sent: the first person who performed the anonymization
evaluation, the immediate superior who reviewed it and finally, the Management Department that
proceeded to review before shipment."

Said manifestation reveals the ignorance of the personnel that has intervened.
nested in the process in relation to the anonymization of the data.

In this sense, it is important to highlight that the data will be considered anonymized in
to the extent that there is no reasonable probability that any person could
identify the natural person in the data set.

The anonymization process is intended to eliminate or minimize the risks
of reidentification of the owners of the data, but without distorting the treatment of
data.

The purpose is to offer greater guarantees of privacy to people, preventing the
breach of confidentiality, integrity and availability of systems and services
treatment rates.

In the present case, the personal data of the complaining party that appear in the
solution attached to the email sent, are not found correctly

minimized allowing the complaining party to be identifiable to persons

who are aware of the non-anonymous circumstances, particularly their place of residence

dence, given the peculiarity of the latter.

For the rest, the way of acting of the staff, as described, involves a

high risk that errors like this can occur.

SESCAM has not contributed to this procedure any document on instructions.

or training their staff in relation to certain practices, such as this one, which

carry a risk of producing a security breach that affects the data

personal.

Moreover, in relation to the measures that it intends to adopt so that it does not happen again.

produce a similar incident in the future, the defendant states that "...the measures to

adopt are those that have been adopted to date: That the documentation passes the

necessary filters to detect that no personal data remains, consider

SENSITIVE..." considering "...the possibility of acquiring an informative program

specific code to facilitate this anonymization of data..." highlighting that the same

would be "... only to facilitate their work to the people who carry out this an-

minimization…" not raised; in any case, the need to delve into the form-

training of your staff in relation to anonymization processes and tools,

so that incidents like the one that occurred do not happen again in the future.

Classification of the infringement of article 32 of the GDPR

SAW

The aforementioned infringement of article 32 of the RGPD supposes the commission of infringements ti-

classified in article 83.4 of the GDPR that under the heading "General conditions for

the imposition of administrative fines" provides:

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

paragraph 2, with administrative fines of a maximum of 10,000,000 EUR or, in the case of

of a company, of an amount equivalent to a maximum of 2% of the volume of

overall annual total business of the previous financial year, opting for the one with the highest

amount:

5)

the obligations of the controller and the person in charge under articles 8,

11, 25 to 39, 42 and 43; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that "Consti-

The acts and behaviors referred to in sections 4, 5 and 6 have infractions

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

the present organic law".

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in article 83.4 of Regulation (EU) 2016/679, the

They are considered serious and will prescribe after two years the infractions that suppose a vulnerability.

substantial portion of the articles mentioned therein and, in particular, the following:

…

f) The lack of adoption of those technical and organizational measures that

are appropriate to guarantee a level of security appropriate to the risk

of the treatment, in the terms required by article 32.1 of the Regulation

(EU) 2016/679. (…)".

Penalty for violation of article 32 of the GDPR

VII

Article 83 "General conditions for the imposition of administrative fines" of the

GDPR section 7 establishes:

"Without prejudice to the corrective powers of the control authorities under art.

Article 58(2), each Member State may lay down rules on whether

of, and to what extent, imposing administrative fines on public authorities and bodies

public establishments established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of liability"

responsible or responsible for the treatment" of the LOPDGDD provides the following:

1. The regime established in this article will be applicable to the treatment of

who are responsible or in charge: ...

c) The General State Administration, the Administrations of the communi-

autonomous entities and the entities that make up the Local Administration…

2. When the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this organic law

only, the data protection authority that is competent will issue a resolution

sanctioning them with warning. The resolution will also establish the

measures that should be adopted to cease the conduct or to correct the effects of the

offense that was committed.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

enough evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on the disciplinary or sanctioning regime that

be applicable.

Likewise, when the infractions are attributable to authorities and executives, and

accredit the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution in which the

sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or regional Gazette that

corresponds.

4. The data protection authority must be informed of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article. (…)"

VIII

Measures

Article 58.2 of the GDPR provides: "Each control authority will have all the

following corrective powers indicated below:

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

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

in a certain way and within a specified period…".

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the

GDPR and order SESCAM to, within three months, establish the measures

adequate security so that the treatments are adapted to the requirements

contemplated in articles 5.1 f) and 32 of the GDPR, preventing the occurrence of

similar situations in the future.

The text of the resolution establishes which have been the infractions committed and the facts that have given rise to the violation of the regulations for the protection of data, from which it is clearly inferred what are the measures to adopt, without prejudice

that the type of procedures, mechanisms or concrete instruments for implement them corresponds to the sanctioned party, since it is responsible for the treatment who fully knows its organization and has to decide, based on the proactive responsibility and risk approach, how to comply with the GDPR and the LOPDGDD, reporting all this to this body.

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 the HEALTH SERVICE OF CASTILLA-LA MANCHA, with NIF Q4500146H, for a violation of Article 5.1.f) of the GDPR, typified in article 83.5 of the GDPR, a warning sanction.

TO IMPOSE the HEALTH SERVICE OF CASTILLA-LA MANCHA, with NIF and, for a infringement of Article 32 of the GDPR, typified in article 83.4 of the GDPR, a warning sanction.

SECOND: REQUEST the CASTILLA-LA MANCHA HEALTH SERVICE to implement, within a period of three months, the necessary corrective measures to adapt their performance to the personal data protection regulations, which prevent that in the

similar events are repeated in the future, as well as to inform this Agency in the same

term

taken.

measures

about

the

THIRD: NOTIFY this resolution to HEALTH SERVICE OF

CASTILLA LA MANCHA.

FOURTH: COMMUNICATE this resolution to the Ombudsman, in

in accordance with the provisions of article 77.5 of the LOPDGDD.

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/11

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

web/], or through any of the other registries provided for in art. 16.4 of the

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

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es