File No.: PS/00293/2022

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the complaining party) dated March 3, 2021

filed a claim with the Spanish Data Protection Agency.

The claim is directed against HEALTH SERVICE OF CASTILLA LA MANCHA

with NIF Q4500146H (hereinafter, the claimed party).

The claim is based on the fact that the claimant, who works as a healthcare professional

in the hospital center ***HOSPITAL.1, denounces that ***PUESTO.1 has sent by

e-mail several service workers a table with your personal information

(name, professional category, results of the Covid-19 tests, if they had

suffered from the disease, and if this had led to sick leave)

- The affected party provides a copy of the email, received on June 3, 2020, and

screenshot of the table attached to it.

Date on which the claimed events took place: June 3, 2020.

Relevant documentation provided by the complaining party:

- copy of the email, received on June 3, 2020, and screenshot of

the attached table.

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

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

hereinafter LOPDGDD), on March 23, 2021, said claim was transferred to

the party claimed, so that it proceeded to its analysis and inform this Agency in the

period of one month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

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 March 24, 2021 as

It is stated in the acknowledgment of receipt that is in the file.

On May 17, 2021, this Agency received a response letter

referring to various documents allegedly incorporated into the brief.

However, since these documents are not included in the brief of

response of the claimed party, these are required, without to date these

have been forwarded.

THIRD: On June 11, 2021, in accordance with article 65 of the

LOPDGDD, the claim filed by the claimant was admitted for processing.

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

question, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

On April 20, 2022, information was requested from the respondent by notification

mail and to the Delegate of Data Protection of the same, by electronic notification.

Both received the notifications without responding to the requests made,

Therefore, on May 18, 2022, the request for information is reiterated, which is

served on May 30, 2022.

The content of the information provided, in essence, is as follows:

“Without prejudice to what corresponds, inform the Coordination and

SESCAM inspection, taking into account the knowledge of the acquired facts

by that body through the "reserved information" processed by said Management in

its day (of which we know that there was a proposal to file by the

Instructing Inspector of the file), I will present the information that we know

following the order of the points proposed by the AEPD itself:

1.- Report of all the actions that have been carried out as a consequence

of the described incident.

(…)

That said, the heads of service and/or section of the 44 medical services that

there are more than 570 area specialists linked to this Management,

have the obligation to organize their respective medical services taking the

corresponding healthcare and organizational decisions. In this line and already in the

period immediately after the declaration of the state of alarm in the State

due to the existence of the pandemic caused by COVID-19, the heads of

medical service adopted measures in their respective services with a double

purpose:

a) Guarantee as much as possible but with total rigor, the prevention of occupational risks of

the medical, health and non-health professionals of the public employees of the

Service, avoiding COVID infections.

b) Guarantee non-delayed continuity of care and minimize the risk of contagion

by COVID of patients. This is the case of the patients of the Oncology Service

radiotherapy that, because they are patients undergoing treatment for cancer, not only are they not

delayed, but require special care in prevention, in this case,

of contagion by COVID-19.

In this sense and for the stated purpose, it should be assessed in the context and

critical situation generated by the pandemic in which this event occurred, should

be assessed if, as understood by this Management, there was legal justification to send the

email with the instructions and/or attached documents that could be

(according to what is said) or data processing, in accordance with the provisions of article 6.1 of the

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

on the protection of natural persons with regard to the processing of

personal information.

(…)

See the obligation imposed on this Management by articles 14 and 15 of the law

31/1995, on occupational risk prevention, as well as the function of the public service

of health with respect to the population served, in accordance with the provisions of Law 14/1986,

General Health and Law 8/2000 of Sanitary Regulation of Castilla-La Mancha; it is

In other words, the need to protect public employees and

the patients cared for.

Well, the existence of an email addressed by B.B.B. What

***POSITION.1 to the doctors of the service and the nursing supervisor, this

Management became aware through a letter dated July 21, 2020

signed by the President of the Board of Personnel of the Health Area of

*** LOCATION.1 giving an account of its existence and of an attached document

in which it is said that the names of employees of the Service of

Radiation oncology and the results of a seroprevalence study,

(…)

However, this Management was never aware of the email and its

content, nor of the document with health data that is said to have been delivered by C.C.C. to

Staff Board;

(...)

2.- Detailed description of the following points:

a) According to the verbal information provided to this Management by ***PUESTO.1, B.B.B., the

email, is used as a means of sending service instructions and

in this case, always according to its manifestation, it was directed exclusively to the

doctors and the nursing supervisor, because on the one hand the doctors are the ones who

They must know which professionals they work with and their situation regarding COVID to

prevent the contagion of patients as the doctor is directly responsible for the

patient during testing and treatment of patients; and the

supervisor as she is the head and responsible for the nursing staff assigned to the

radiation oncology service.

However, as indicated, we do not know the content of the email.

b) If the email was sent without hiding the email addresses

e-mail from the rest of the recipient professionals, this could be due to the

following reasons:

- Be the professional email address, that is, the one used

to issue service instructions, service organization, existing news

in it, not being a private email address.

- Possible need for all recipients to know that the rest of the

recipients are also aware of the message for better organization and work

in equipment belonging to the medical and health profession.

- Because while the private email address can be considered to be

contains personal data, within the scope of SESCAM the corporate addresses of

e-mail must be known by the need for its use between the different

medical and health professionals to communicate with each other.

c) It is to be assumed that the "table" referred to, the content of which is unknown to this

Management, has not been subject to any treatment after its use, but it would be

eliminated once its purpose has been fulfilled. This has been reported to us by ***PUESTO.1

prior to the issuance of this document.

d) No specific security measures have been adopted for an event that we do not

It consists, beyond the periodic information that is transferred to all professionals

on the normative regulation of data processing.

3) If applicable, the reason why the security breach has not been reported to this

Diary.

As can be inferred from the foregoing and especially from what is referred to in point 1 of this

document, this Management was not aware of the existence of the alleged

security breach or incidents that support it according to legal regulation

existing, but in any case, as the President of the Personnel Board was informed,

of actions in the field of medical service management.

(…)

4.- If applicable, information on whether other emails have been sent

similar without a blind copy of the recipients, with or without an attached document with data

personal.

This Management has informed the dependent employees of the same that they must

take extreme precautions not to reveal personal data by any means,

not knowing at this time if there were later similar emails without

blind copy of the recipients, nor of course has it come to our knowledge

complaint arising from similar events.

5- Technical and organizational measures adopted to avoid, as far as possible, incidents of

security like what happened.

The events that the AEPD claims to have occurred cannot be extrapolated to a

situation aside from the serious crisis produced in all the country's hospitals that

meant its collapse and almost impossibility to provide health care. Therefore and to

outside of the information transmitted from our central structures, the facts

that are said to have occurred cannot occur again because they occurred as already

has indicated intimately linked and derived from the pandemic and the collapse

hospitable.

6.- Training plan for health personnel on data protection and

description of the procedure established for the referral of this type of

communications. Copy of the instructions addressed to the personnel in charge of your

Shipping.

Within SESCAM there is an information security committee that marks

guidelines and measures to be adopted, communicated through regular meetings

celebrated with all the Managements.

Along these lines, the ***LOCALIDAD.1 Integrated Attention Management has

developed its own online course on information security

("Information Security. Undue access"), whose deadline for submitting

Instances have already started, with the start of the course scheduled for the first few days

of the month of June 2022 and must be compulsorily completed as a day of

work for the more than 5,000 employees who currently depend on this

Management.

Prior to this, for some years our Central Services have been

organizes a course called "THE PROTECTION OF PERSONAL DATA

EN EL SESCAM", lasting 25 hours, with more than six editions and access

for all SESCAM staff."

In relation to the response of the claimed evacuated within the present

investigative actions and that has been partially transcribed in paragraphs

precedent, it should be noted that:

The documents attached to the brief have not been included in the information provided.

from the Integrated Attention Management of ***LOCALIDAD.1, with which

supposedly it is answered to the transfer of the claim.

The respondent insists that she is unaware of both the e-mail sent, and that

motivates the claim that is now being investigated, as well as the annex attached to it in the

containing data from various service workers: name, category

professional, results of the Covid-19 tests, if they had suffered from the disease,

and if this had led to sick leave.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/17

The following information was found from the mail analysed:

The address from which it was sent is ***EMAIL.1.

The email was addressed to ***EMAIL.2

The recipients in a copy of the mail were:

***EMAIL.3

***EMAIL.4

***EMAIL.5

***EMAIL.6

***EMAIL.7

***EMAIL.8

None of the email recipient addresses are emails

corporate of the claimed. Only the address from which the mail was sent

it is corporate.

The table attached to the mail contains the data of 40 people related to: Employee (with

Name); serological PCR test; Symptoms; sick leave; Category.

The data contained in the table affects personnel of different categories:

Receptionist, Administrative, Gauges, Auxiliary DUE, DUE, TERT, Radiophysicists and

Doctors.

Two relevant aspects emerge from the actions described above:

1.- It has been proven that on June 3, 2020 at 4:20 p.m., the

Radiotherapy Oncology Service of the hospital center ***HOSPITAL.1 sent by

e-mail several service workers a table with your personal information

(name, professional category, results of the Covid-19 tests, if they had

suffered from the disease, and if this had led to sick leave).

The address from which it was sent is ***EMAIL.1.

The email was addressed to ***EMAIL.2

The recipients in a copy of the mail were:

***EMAIL.3

***EMAIL.4

***EMAIL.5

***EMAIL.6

***EMAIL.7

***EMAIL.8

None of the email recipient addresses are emails

corporate of the claimed. Only the address from which the mail was sent

it is corporate.

The table attached to the mail contains the data of 40 people related to: Employee (with

Name); serological PCR test; Symptoms; sick leave; Category.

2.- Regarding the breach of confidentiality, it is verified that it has not been notified to the

Spanish Data Protection Agency. There is not enough evidence

about the rest of the information regarding the gap and specifically the destination that has been

given to the data contained in the table and whether they have been deleted or not.

FIFTH: On June 2, 2022, the Director of the Spanish Agency for

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

for the alleged infringement of article 5.1.f) of the RGPD, article 9 of the RGPD and article

32 of the RGPD, typified in article 83.5 of the RGPD.

SIXTH: On June 24, 2022, the entity claimed in response to the agreement

beginning of this sanctioning procedure, reiterates the statements made on

May 30, 2022, indicated in the fourth antecedent, on the occasion of the

request for information made in the phase of actions prior to the start of this

procedure, establishing the following nuances on the alleged

penalties charged:

In relation to the alleged sanction of article 5.1 f) of the RGPD, the entity claimed

considers that the incorporation of the data was intended to guarantee the security

of the patients and that of the rest of the employees of the oncology and radiotherapy service.

Regarding the alleged sanction of article 9 of the RGPD, the entity claimed

considers that the disclosed information does not indicate any health data, only if the

workers as a result of having suffered from the COVID disease, had

generated or not antibodies.

Regarding the alleged sanction of article 32 of the RGPD, the entity claimed

states that it has not declared the security breach because it was not known

of it until it has become aware of this complaint.

SEVENTH: On July 8, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

address a warning to the HEALTH SERVICE OF CASTILLA LA MANCHA, with

NIF Q4500146H, for an infringement of article 5.1.f) of the RGPD, a second

infringement of article 9 of the RGPD typified both in article 83.5 of the RGPD and

a third infringement of article 32 of the RGPD, typified in article 83.4 of the

GDPR.

EIGHTH: On July 27, 2022, arguments are presented to the proposal for

resolution, in the same sense as in the allegations to the initial agreement, affirming

Specifically, the alleged facts are based on the following:

".-That there was a legal obligation to act in the way that was done, for reasons of

safety and health of patients and workers of the Radiotherapy Service.

- That the information was given to the reduced group of doctors of the Service and

Nursing supervisor who have the responsibility to fulfill such tasks.

- That the document in question was used for a single purpose and was destroyed

later without being incorporated into a data base with a vocation for permanence.

- That the document remained in the custody of the Personnel Board without this

Management was given transfer of the same, not being able to adopt any measure

nor communicate the alleged security breach. to exist.

- That there was no security breach."

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

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: On June 3, 2020, an email is sent by the entity

claimed to several workers in which personal information appeared (name,

professional category, results of the Covid-19 tests, if they had suffered from the

illness, and if this had led to sick leave)

SECOND: On June 24, 2020, the respondent entity presents allegations

stating that their action is justified for security reasons, that the data

were relative to whether the patients had generated antibodies from having suffered

COVID, and that the security breach was not declared due to not having knowledge of the

same.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control, and according to the provisions of articles 47 and 48 of the LOPDGDD, the Director

of the Spanish Agency for Data Protection is competent to initiate and to

resolve this procedure.

II

The principles relating to the processing of personal data are regulated in the

Article 5 of the RGPD where it is established that “personal data will be:

“a) processed in a lawful, loyal and transparent manner in relation to the interested party (“lawfulness,

loyalty and transparency»);

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with those purposes; according to article 89,

paragraph 1, the further processing of personal data for archiving purposes in

public interest, scientific and historical research purposes or statistical purposes are not

deemed incompatible with the original purposes ("purpose limitation");

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which

that are processed ("data minimization");

d) accurate and, if necessary, updated; all measures will be taken

reasonable to eliminate or rectify without delay the personal data that

are inaccurate with respect to the purposes for which they are processed (“accuracy”);

e) kept in a way that allows the identification of the interested parties during

longer than necessary for the purposes of the processing of personal data; the

Personal data may be kept for longer periods provided that it is

processed exclusively for archival purposes in the public interest, research purposes

scientific or historical or statistical purposes, in accordance with Article 89, paragraph 1,

without prejudice to the application of the appropriate technical and organizational measures that

This Regulation is imposed in order to protect the rights and freedoms of the

interested party (“limitation of the retention period”);

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

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational ("integrity and confidentiality").

The data controller will be responsible for compliance with the provisions of

section 1 and able to demonstrate it (“proactive responsibility”).”

The infringement of art. 5.1.f) is typified in article 83.5 of the RGPD which provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the

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; (…)"

Article 72.1 a) of the LOPDGDD states that "according to what is established in 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".

III

We must also take into account that article 9 of the RGPD establishes the following:

1. The processing of personal data that reveals ethnic origin is prohibited

or racial background, political opinions, religious or philosophical convictions, or affiliation

union, and the processing of genetic data, biometric data aimed at identifying

unambiguously to a natural person, data relating to health or data relating to

sexual life or sexual orientations of a natural person.

2. Section 1 shall not apply when one of the following circumstances occurs-

following:

a) the interested party gave their explicit consent for the processing of said data

for one or more of the specified purposes, except when the Right of

the Union or the Member States establishes that the prohibition referred to in the

section 1 cannot be lifted by the interested party;

b) the treatment is necessary for the fulfillment of obligations and the exercise of

specific rights of the person in charge of the treatment or of the interested party in the field of

Labor law and security and social protection, to the extent that it is so authorized.

enact the Law of the Union of the Member States or a collective agreement with

under the Law of the Member States that establishes adequate guarantees of the res-

protection of the fundamental rights and interests of the interested party;

c) the treatment is necessary to protect the vital interests of the interested party or another

natural person, in the event that the interested party is not qualified, natural or legal,

cally, to give your consent;

d) the treatment is carried out, within the scope of its legitimate activities and with the de-

guarantees, by a foundation, an association or any other organization without

for profit, whose purpose is political, philosophical, religious or trade union, provided that the

treatment refers exclusively to current or former members of such organizations.

organizations or persons who maintain regular contact with them in relation to

its purposes and provided that the personal data is not communicated outside of them without the

consent of the interested parties;

e) the treatment refers to personal data that the interested party has made manifest-

public mind;

f) the treatment is necessary for the formulation, exercise or defense of claims.

tions or when the courts act in the exercise of their judicial function;

g) the treatment is necessary for reasons of an essential public interest, on the

basis of the law of the Union or of the Member States, which must be proportional

the objective pursued, essentially respect the right to data protection and

establish adequate and specific measures to protect the interests and rights

fundamentals of the interested party;

h) the treatment is necessary for the purposes of preventive or occupational medicine, evaluation

of the worker's work capacity, medical diagnosis, provision of assistance or

treatment of a health or social nature, or management of health care systems and services.

health and social care, on the basis of the Law of the Union or of the Member States.

or by virtue of a contract with a healthcare professional and without prejudice to the conditions

tions and guarantees contemplated in section 3;

i) the treatment is necessary for reasons of public interest in the field of health

such as protection against serious cross-border threats to health, or

to ensure high levels of quality and safety of healthcare and

of medicines or medical devices, on the basis of Union Law or

of the Member States to establish appropriate and specific measures to pro-

protect the rights and freedoms of the interested party, in particular professional secrecy,

j) the processing is necessary for archiving purposes in the public interest, research purposes,

scientific or historical information or statistical purposes, in accordance with article 89,

paragraph 1, on the basis of the law of the Union or of the Member States, which

must be proportional to the objective pursued, respect essentially the right to

data protection and establish adequate and specific measures to protect the

interests and fundamental rights of the interested party.

3. The personal data referred to in section 1 may be processed for the purposes cited-

two in section 2, letter h), when their treatment is carried out by a professional

subject to the obligation of professional secrecy, or under your responsibility, in accordance

with the Law of the Union or of the Member States or with the established rules

by the competent national bodies, or by any other person also subject to

also to the obligation of secrecy in accordance with the Law of the Union or of the States.

two members or of the standards established by the competent national bodies.

you.

4. Member States may maintain or introduce additional conditions, including

ive limitations, with respect to the processing of genetic data, biometric data or

health-related data.

The infringement of article 9 of the RGPD is provided for in article 83.5 of the RGPD

where it is established that:

“The infractions of the following dispositions will be sanctioned, in accordance with the

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

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

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

amount:

a)

consent under articles 5,6,7 and 9.”

The basic principles for the treatment, including the conditions for the

In turn, the LOPDGDD in its article 72.1.e) qualifies as a very serious infraction,

purposes of prescription, “The treatment of personal data of the categories to which

referred to in article 9 of Regulation (EU) 2016/679 without any of the

the circumstances provided for in said precept and in the article of this Organic Law.”

IV

Security in the processing of personal data is regulated in article 32 of the

RGPD where the following is established:

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

nature, scope, context and purposes of the treatment, as well as risks of probability

variable and seriousness for the rights and freedoms of natural persons, the responsible

The controller and the data processor will apply appropriate technical and organizational measures.

to guarantee a level of security appropriate to the risk, which, where appropriate, includes

yeah, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

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

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the treatment.

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

ta the risks that the treatment of data presents, in particular as a consequence

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

stored, stored or otherwise processed, or unauthorized communication or access

two to said data.

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

certification body approved under article 42 may serve as an element for

demonstrate compliance with the requirements established in section 1 of this

Article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that

Any person acting under the authority of the person in charge or the person in charge and having

access to personal data can only process said data following instructions

of the person in charge, unless it is obliged to do so by virtue of Union Law or

member states."

The infringement of article 32 of the RGPD is typified in article 83.4 of the RGPD that under

the heading "General conditions for the imposition of administrative fines" has

ne:

"The infractions of the following dispositions will be sanctioned, in accordance with the

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

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

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

the largest amount:

a) the obligations of the person in charge and of the person in charge in accordance with articles 8, 11, 25 to

39, 42 and 43."

Article 73.f) of the LOPDGDD, under the heading "Infringements considered serious

has:

"According to article 83.4 of Regulation (EU) 2016/679, they will be considered serious and

Infractions that suppose a substantial violation will prescribe after two years.

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

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

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679

v

The LOPDGDD in its article 77, Regime applicable to certain categories of

responsible or in charge of the treatment, establishes the following:

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

who are responsible or in charge:

a) The constitutional bodies or those with constitutional relevance and the institutions of

autonomous communities analogous to them.

b) The jurisdictional bodies.

c) The General Administration of the State, the Administrations of the communities

autonomous and the entities that make up the Local Administration.

d) Public bodies and public law entities linked or

dependent on the Public Administrations.

e) The independent administrative authorities.

f) The Bank of Spain.

g) Public law corporations when the purposes of the treatment are

related to the exercise of powers of public law.

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Legislative Assemblies

autonomous, as well as the political groups of the Local Corporations.

2. When those responsible or in charge listed in section 1 committed
any of the infractions referred to in articles 72 to 74 of this law
organic, the data protection authority that is competent will dictate
resolution sanctioning them with a warning. The resolution will establish
also the measures that should be adopted to stop the behavior or correct it.
the effects of the infraction that had been committed.
The resolution will be notified to the person in charge or in charge of the treatment, to the body of the
that depends hierarchically, where appropriate, and to those affected who had the condition
interested party, if any.
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
sufficient evidence for it. In this case, the procedure and the sanctions to be applied
will be those established in the legislation on disciplinary or sanctioning regime that
result of application.
Likewise, when the infractions are attributable to authorities and managers, and
proves the existence of technical reports or recommendations for the treatment that
had not been duly attended to, in the resolution imposing the
The sanction will include a reprimand with the name of the responsible position and
will order the publication in the Official State or Autonomous Gazette that
correspond.
4. The data protection authority must be notified 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.

6. When the competent authority is the Spanish Data Protection Agency,

this will publish on its website with due separation the resolutions referring to

the entities of section 1 of this article, with express indication of the identity

of the person in charge or in charge of the treatment that had committed the infraction.

When the competence corresponds to a regional authority for the protection of

data will be, in terms of the publicity of these resolutions, to what your

specific regulations".

SAW

Article 58.2 of the RGPD provides the following: "Each control authority will have

of all the following corrective powers indicated below:

b) direct any person responsible or in charge of the treatment with a warning when

treatment operations have violated the provisions of this

Regulation;

d) order the person in charge or 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;

i) impose an administrative fine under article 83, in addition to or instead of

the measures mentioned in this section, according to the circumstances of each

particular case;

7th

A claim is filed for the referral of e-mail by the entity

claimed to several workers in which personal information appeared (name,

professional category, results of COVID-19 tests, if they had suffered from the

illness, and if this had led to sick leave)

In writing of allegations both in the initial agreement and in the proposal for

resolution, the defendant entity justifies the imputed facts alleging reasons of

public safety, and that the information provided was solely about whether some

workers had or had not generated antibodies after having suffered from COVID-19, as well

such as the impossibility of communicating the security breach due to ignorance.

Specifically, it justifies its action by alleging the following:

".-That there was a legal obligation to act in the way that was done, for reasons of

safety and health of patients and workers of the Radiotherapy Service.

- That the information was given to the reduced group of doctors of the Service and

Nursing supervisor who have the responsibility to fulfill such tasks.

- That the document in question was used for a single purpose and was destroyed

later without being incorporated into a data base with a vocation for permanence.

- That the document remained in the custody of the Personnel Board without this

Management was given transfer of the same, not being able to adopt any measure

nor communicate the alleged security breach if it exists.

- That there was no security breach."

In accordance with the evidence available, it is found that the email

object of conflict contained a table with your personal information (name, category

professional, results of the Covid-19 tests, if they had suffered from the disease,

and if this had led to sick leave), which contravenes article 9 of the RGPD,

since the claimed entity has processed the health data of the

claimant, without being in any of the cases indicated in article 9.2 of the

RGPD, as indicated in the legal basis III.

It is also considered the commission of the infringement of article 5.1 f) of the RGPD, which

The principle of integrity and confidentiality governs, so that the data is treated in a

in such a way as to ensure adequate security of personal data, including

protection against unauthorized or unlawful processing and against loss,

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

appropriate organisations.

Regarding the breach of confidentiality produced, it is verified that it has not been

notified to the Spanish Data Protection Agency.

There is insufficient evidence on the rest of the information regarding the

gap and specifically the destination that has been given to the data contained in the table and if

these have been suppressed or not.

This Agency considers that the security measures of the claimed entity do not

were adequate at the time of the incident that is the subject of the claim and

must be improved because it is confirmed that they have not been sufficient to prevent

the reported facts.

Thus, this Agency considers that the claimed entity has violated the

articles 9, 5.1 f) and 32 of the RGPD, when treating health data, especially protected,

secondly for violating the principle of integrity and confidentiality, and finally

for not adopting the necessary security measures to guarantee the protection of

the personal data of your staff.

viii

The text of the resolution establishes 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 measures to adopt, without prejudice

that the type of specific procedures, mechanisms or instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

treatment who fully knows your organization and has to decide, based on the

proactive responsibility and risk approach, how to comply with the RGPD and the

LOPDGDD.

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

graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the HEALTH SERVICE OF CASTILLA LA MANCHA, with

NIF Q4500146H, for an infringement of article 5.1.f) of the RGPD, typified in the

article 83.5 of the RGPD, a sanction of warning.

SECOND: IMPOSE the HEALTH SERVICE OF CASTILLA LA MANCHA, with

NIF Q4500146H, for an infringement of article 9 of the RGPD, typified in article

83.5 of the RGPD, a sanction of warning.

THIRD: IMPOSE the HEALTH SERVICE OF CASTILLA LA MANCHA, with

NIF Q4500146H, for an infringement of article 32 of the RGPD, typified in article

83.4 of the RGPD, a sanction of warning.

FOURTH: THAT the HEALTH SERVICE OF CASTILLA LA MANCHA adopt the

necessary measures for proper treatment of health data, as well as

measures that guarantee the integrity, confidentiality and security of the data

treated personal, as well as the provision of means of proof accrediting the

compliance with the requirements within a month from the notification of the

this resolution.

FIFTH: COMMUNICATE this resolution to the Ombudsman, in accordance

with the provisions of article 77.5 of the LOPDGDD.

SIXTH: NOTIFY this resolution to the CASTILLA HEALTH SERVICE

THE STAIN.

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

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

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

938-120722

www.aepd.es

sedeagpd.gob.es