 File No.: EXP202205570

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), on May 9, 2022,

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the CANARIAN HEALTH SERVICE with NIF

Q8555011I (hereinafter, the claimed party). The reasons on which the claim is based

are the following:

He claims to have been given, for signature, a document called

Notification of Registration on the Surgical Waiting List, which contains the data

another patient's personal Provide a copy of the aforementioned document.

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

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the claimed party,

to proceed with its analysis and inform this Agency within a month,

of the actions carried out to adapt to the requirements established 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), by means of electronic notification, was received in

dated May 19, 2022, as stated in the certificate in the file.

No response has been received to this letter of transfer.

THIRD: On August 3, 2022, in accordance with article 65 of the

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

FOURTH: On November 4, 2022, the Director of the Spanish Agency for

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

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

of the Common Administrative Procedure of Public Administrations (in

hereinafter, LPACAP), for the alleged infringement of article 5.1.f) of the GDPR and article

32 of the GDPR, typified in articles 83.5 of and 83.4 of the GDPR, respectively.

The initiation agreement was notified, in accordance with the regulations established in the Law

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

Public Administrations (hereinafter, LPACAP), on November 9, 2022,

as stated in the certificate that is in the file.

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), the claimed party submitted a written

of allegations in which, in summary, he stated that there was a problem of

paperwork in the printer and, by mistake, the documentation was given to you for your signature

concerning another patient who had also been sent to print at that time. He

staff immediately realized the error and after locating the patient they were summoned

again in successive consultation to give you the pertinent explanations, apologize

with him and proceed to sign the correct documentation issued in his name.

It considers that in no case has there been improper access to the clinical history of

none of the patients involved, all confusion being due to human error in

the collection of documents in the printer.

Regarding the measures adopted to avoid this type of confusion, he states

that all the personnel of the Canary Islands Health Service are informed of the good

information security practices.

As an additional security measure, it is reported that the

installation of multifunctional printers with secure printing in the Hospital

involved, so the document is not printed until the person enters

your print code on the printer, so that, when the person in question is there,

said moment, you can pick up the printed document directly, without having to

opportunity to pick up a document that is not yours.

SIXTH: On January 9, 2023, a resolution proposal was formulated,

proposing:

<< That by the Director of the Spanish Agency for Data Protection be imposed on the

CANARIAN HEALTH SERVICE, with NIF Q8555011I,

-for an infringement of article 5.1.f) of the GDPR, classified in accordance with the provisions of article

Article 83.5 of the GDPR, classified as very serious for the purposes of prescription in the

Article 72.1 a) of the LOPDGDD, a warning sanction.

- for a violation of article 32 of the GDPR, classified in accordance with the provisions of article

article 83.4 of the GDPR, classified as serious for the purposes of prescription in article

73 f) of the LOPDGDD, a warning sanction.>>

The aforementioned resolution proposal was sent, in accordance with the rules established in

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

Public Administrations (hereinafter, LPACAP), by means of electronic notification,

being received on January 10, 2023, as stated in the certificate that works

on the record.

SEVENTH: The claimed party has not submitted allegations to the Proposal for

Resolution.

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: On May 9, 2022, the claimant filed a writ of

claim before the Spanish Data Protection Agency (AEPD), in which

expressed his disagreement with the reception for his signature, of a document

called Notification of Registration on the Surgical Waiting List, which included

the personal data of another patient.

SECOND: Once the documentation provided has been verified and that it is incorporated

to the file, there is evidence that a document called Notification of Registration in the List of

Surgical Waiting, which contains the personal data of another patient, has been

signed by the claimant, allowing unauthorized access by a third party.

THIRD: The claimed party acknowledges that the incident that is the subject of the claim was

due to a human error in the collection of the documents in the printer and exposes

that the installation of multifunctional printers with

Secure printing at the Hospital involved.

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."

In response to the allegations presented by the respondent entity, it should be noted

the next:

II

In the first place, it has been verified that the security measures available

implanted the claimed party in relation to the data that was subjected to treatment in

responsible, were not adequate at the time of the bankruptcy

security of personal data, with the consequence of access by a third party outside

personal information.

Security measures must be adopted in attention to each and every one of the

risks present in the processing of personal data, including among

the same, the human factor.

The facts proven in the procedure show that the claimant has agreed
improperly to personal data of another patient with breach of the
technical and organizational measures and violating the confidentiality of the data.
In addition, the category of data to which the claimant has had access is
in the category of specials according to the provisions of art. 9 of the GDPR, circumstance
that implies an added risk that must be assessed in the risk management study
and that the requirement of the degree of protection in relation to the security and
safeguarding the integrity and confidentiality of this data.
However, it should be noted that technical and organizational security measures
being implemented by the respondent entity are reasonable and adequate for the
estimated risk level.
Consequently, the allegations must be dismissed, meaning that the
arguments presented do not distort the essential content of the offense that
is declared committed nor does it imply sufficient justification or exculpation.

II

Regarding the health data, recital 35 of the GDPR indicates:
“Personal data relating to health should include all personal data
relating to the state of health of the interested party that provide information about their state of
past, present or future physical or mental health. Information is included about the
natural person collected on the occasion of your registration for the purposes of health care,
or on the occasion of the provision of such assistance, in accordance with Directive
2011/24/EU of the European Parliament and of the Council; any number, symbol or data
assigned to a natural person who uniquely identifies them for the purposes of
sanitary; information obtained from tests or examinations of a part of the body or
of a body substance, including from genetic data and samples

biological, and any information related, by way of example, to a disease, a

disability, disease risk, medical history, treatment

clinical or physiological or biomedical state of the data subject, regardless of their

source, for example a doctor or other healthcare professional, a hospital, a device

physician, or an in vitro diagnostic test.”

Article 4 of the GDPR defines:

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

covers personal data or sets of personal data, either by automated procedures

tomatoized or not, such as the collection, registration, organization, structuring, conservation

tion, adaptation or modification, extraction, consultation, use, communication by

transmission, diffusion or any other form of authorization of access, collation or interco-

connection, limitation, suppression or destruction;”

7) "responsible for the treatment" or "responsible": the natural or legal person,

public authority, service or other body which, alone or jointly with others, determines the

purposes and means of processing; if the law of the Union or of the Member States

determines the purposes and means of processing, the controller or the

Specific criteria for their appointment may be established by Union law

or of the Member States;

10) "third party": natural or legal person, public authority, service or body

other than the interested party, the person in charge of the treatment, the person in charge of the treatment

and of the persons authorized to process the personal data under the direct authority

of the person in charge or of the person in charge;

IV.

Law 41/2002, of November 14, basic regulation of patient autonomy

and rights and obligations regarding clinical information and documentation (in

hereafter, LAP), establishes in its Preamble that: "the healthcare organization must

allow guaranteeing health as an inalienable right of the population through the

structure of the National Health System, which must be ensured in conditions of

scrupulous respect for personal privacy and the individual freedom of the user,

guaranteeing the confidentiality of information related to the services

health services that are provided and without any type of discrimination".

In this sense, the LAP defines in article 3 that the clinical history is: "the set of

documents containing the data, assessments and information of any kind

about the situation and clinical evolution of a patient throughout the care process.

cial".

Article 14 of the LAP indicates:

"1. The clinical history comprises the set of documents related to the procedures

care of each patient, with the identification of the doctors and the de-

more professionals who have intervened in them, in order to obtain the maximum interest

possible gradation of the clinical documentation of each patient, at least, in the field

from each center.

2. Each center will file the medical records of its patients, anyone who

be it the paper, audiovisual, computer or other type of support in which they are recorded, in

in such a way that their safety, correct conservation and recovery are guaranteed.

tion of information."

In this way, all professionals who intervene in the care activity are obliged to

compliance with the duties of information and clinical documentation, in such a way that

so that the dignity of the human person, respect for the autonomy of his will

and to their privacy, they will guide all the activity aimed at obtaining, using, filing,

custody and transmission of clinical information and documentation.

Thus, it can be deduced that the health services must generate and guard the respective

Unique medical records per patient and service.

In this sense, article 17.6 of the LAP, dedicated to the preservation of documents

clinical station, indicates:

“The technical safety measures are applicable to clinical documentation.

established by the legislation regulating the conservation of the files that

contain personal data and, in general, by Organic Law 15/1999, of

Personal data protection."

And article 19 establishes as a right related to the custody of history that:

“The patient has the right for health centers to establish a mechanism for

active and diligent custody of medical records. Said custody will allow the collection

da, integration, retrieval and communication of information submitted to the

principle of confidentiality in accordance with the provisions of article 16 of the pre-

sente Law.”

V

Article 5.1.f) of the GDPR

Article 5.1.f) of the GDPR establishes the following:

"Article 5 Principles relating to treatment:

1. Personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing and against

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

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

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the GDPR, principles relating to treatment, all

time the claimant has improperly accessed personal data of another

patient, violating the principles of integrity and confidentiality, both

established in the aforementioned article 5.1.f) of the GDPR.

As proven in the file, it is clear that a document called

Notification of Registration on the Surgical Waiting List, which contains the data

personal information of another patient, has been signed by the claimant, allowing access

not authorized by a third party.

The person responsible for the treatment of the data that forms part of the clinical history is the

health Center. The latter has the obligation to prepare it, guard it and implement the measures

necessary security measures so that it is not lost, is not communicated to unauthorized parties

interested or can be accessed by unauthorized third parties.

Consequently, it is considered that the accredited facts are constitutive of

infringement, attributable to the claimed party, due to violation of article 5.1.f) of the

GDPR.

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

SAW

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/12

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 maximum EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the total annual global business volume of the previous financial year, opting for the highest amount:

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

consent 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 result contrary to this organic law".

For the purposes of the limitation period, article 72 "Infractions considered very serious" 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 in article 5 of Regulation (EU) 2016/679. (…)"

VII

GDPR Article 32

Article 32 of the GDPR, security of treatment, establishes the following:

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

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

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the pseudonymization and encryption of personal data;

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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

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

2. When evaluating the adequacy of the level of security, particular attention should be paid to

take into account the risks presented by data processing, in particular as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to said data (The underlining is from the AEPD).

Recital 75 of the GDPR lists a series of factors or assumptions associated with

risks to the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and

variable probability, may be due to data processing that could cause

physical, material or immaterial damages and losses, particularly in cases in which

that the treatment may give rise to problems of discrimination, usurpation of

identity or fraud, financial loss, damage to reputation, loss of

confidentiality of data subject to professional secrecy, unauthorized reversal of the

pseudonymization or any other significant economic or social harm; in the

cases in which the interested parties are deprived of their rights and freedoms or are

prevent you from exercising control over your personal data; In cases where the data

personal treaties reveal ethnic or racial origin, political opinions, religion

or philosophical beliefs, union membership and genetic data processing,

data relating to health or data on sexual life, or convictions and offenses

criminal or related security measures; in cases where they are evaluated

personal aspects, in particular the analysis or prediction of aspects related to the

performance at work, economic situation, health, preferences or interests

personal, reliability or behavior, situation or movements, in order to create or

use personal profiles; in cases in which personal data of

vulnerable people, particularly children; or in cases where the treatment

involves a large amount of personal data and affects a large number of

interested.”

The facts revealed imply the lack of technical measures and

organizational measures to guarantee the confidentiality of the personal data object of

treatment, by disseminating a document that contained personal data of another

patient with the consequent lack of diligence by the person in charge, allowing the

unauthorized access by third parties.

This conduct of the claimed evidence that he did not adopt the organizational measures

necessary to guarantee the security of the personal data that it processes,

thus breaching the obligation that article 32 of the GDPR imposes.

From the actions carried out, there is evidence of the existence of reasonable and

enough that security measures, both technical and

organizations, with which the claimed party had in relation to the data of

health, were not adequate at the time of the improper access.

The consequence of this implementation of deficient security measures was the

exposure to a third party of the personal data related to the health of another

patient. In other words, the affected party has been deprived of control over their data

Personal data relating to your medical history.

It should be added that, in relation to the category of data to which a third party

someone else has had access, they are in the special category according to what

provided in art. 9 of the GDPR, a circumstance that implies an added risk that is

must be assessed in the risk management study and that the degree requirement increases

of protection in relation to the security and safeguarding of the integrity and

confidentiality of these data.

This risk must be taken into account by the controller who must

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the person responsible for the treatment and, therefore, by the

holders of the data that provided them.

Classification of the infringement of article 32 of the GDPR

VIII

The aforementioned infringement of article 32 of the GDPR supposes the commission of the infringements

typified 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 maximum EUR 10,000,000 or,

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

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

the highest amount:

to)

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

"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 result

contrary to this 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,

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

substantial violation 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 ensure a level of security appropriate to the

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

Regulation (EU) 2016/679."

IX

Responsibility

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/12

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III relating to the "Principles of the Power to sanction", in article 28

under the heading "Responsibility", the following:

"1. They may only be penalized for acts constituting an administrative offense

physical and legal persons, as well as, when a Law recognizes their capacity to

act, the affected groups, the unions and entities without legal personality and the

independent or autonomous patrimonies, which are responsible for them

title of fraud or fault."

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

with the consequence of the breach of the principle of confidentiality constitutes the

element of guilt.

X

Sanction

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

GDPR in its section 7 establishes:

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

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

can, and to what extent, impose administrative fines on authorities and bodies

public establishments established in that Member State."

The Spanish legal system has chosen not to penalize entities

public but with a warning, as indicated in article 77.1. c) and 2. 4. 5. and 6.

of the LOPDGDD:

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

who are responsible or in charge:

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

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 law

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

likewise, the measures that should be adopted to cease the conduct or to correct it.

the effects of the offense 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, 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

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.

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 infringement.

When the competence corresponds to an autonomous authority for the protection of

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

specific regulations."

In the present case, from the solid evidence available in accordance with the facts proven in this disciplinary proceeding, it is deemed appropriate sanction the claimed party with a warning for violation of article 5.1.f) of the GDPR and for the infringement of article 32 of the GDPR, for 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 with the consequence of the breach of the principle of confidentiality.

eleventh

Measures

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.

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: SANCTION the CANARIAN SERVICE OF THE SALUD, with NIF Q8555011I, for a violation of article 5.1.f) of the GDPR, typified in article 83.5 of the GDPR.

SECOND: SANCTION the CANARIAN SERVICE OF THE

SALUD, with NIF Q8555011I, for a violation of article 32 of the GDPR, typified in

Article 83.4 of the GDPR.

THIRD: REQUEST the CANARIAN HEALTH SERVICE, with NIF Q8555011I,

to implement, within three months, the necessary corrective measures to

adapt their actions to the personal data protection regulations, which prevent

that in the future similar events are repeated, such as the installation of printers

multifunctional printers with secure printing, as well as to inform this Agency in the

same term on the measures adopted.

FOURTH: NOTIFY this resolution to the CANARY HEALTH SERVICE.

FIFTH: COMMUNICATE this resolution to the Ombudsman, 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

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