 Procedure No.: PS/00443/2019

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the claimant) dated June 5, 2019

filed a claim with the Spanish Data Protection Agency. The

claim is directed against ANDALUZ HEALTH SERVICE with NIF Q9150013B

(hereinafter, the claimed). The grounds on which the claim is based are, in short,

that on 04/16/2019 he requested his medical history and was told that it was not

they can facilitate because it has been lost due to moving; you requested

the supporting document of such circumstance up to two times and finally

they sent it. Attach this document.

SECOND: Upon receipt of the claim, the Subdirectorate General for

Data Inspection proceeded to carry out the following actions:

On 07/22/2019, the brief filed was transferred to the defendant for analysis and

communication to the complainant of the decision adopted in this regard. Likewise, it

required so that within a month it would send to the Agency determined

information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant.

On 08/02/2019, the respondent responded to the request for information stating

that the request for documentation of the claimant's medical history was requested from the

Regional Hospital of ***LOCATION.1, to the Management Office of the aforementioned

hospital center report of the reasons that have caused the claim made

before the AEPD, stating:

1.- That they have carried out an exhaustive search of the requested documents

by the interested party, from which a negative response has been obtained.

2.- That they do not exist in the databases or in the files of the Hospital

Regional of *** LOCATION.1, any record of actions and/or attentions

made to the claimant before 2007.

3.- That all the documentation generated from 2007 has been delivered

to the claimant.

THIRD: On 11/26/2019, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed by the claimant against the respondent.

FOURTH: On 12/18/2019, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

infringement of article 32 of the RGPD, typified in article 63.4.a) of the aforementioned

Regulation., considering that the sanction that could correspond would be

WARNING.

FIFTH: Once the initiation agreement has been notified, the one claimed at the time of this
The resolution has not presented a written statement of allegations, for which reason the
indicated in article 64 of Law 39/2015, of October 1, on the Procedure
Common Administrative Law of Public Administrations, which in section f)
establishes that in the event of not making allegations within the period established on the
content of the initiation agreement, it may be considered a proposal for
resolution when it contains a precise statement about the responsibility
imputed, reason why a Resolution is issued.

SIXTH: Of the actions carried out in this proceeding, they have been
accredited the following:

PROVEN FACTS

FIRST: On 06/05/2019 there is an entry in the AEPD written by the claimant indicating
that on 04/16/2019 he requested his clinical history from the Regional Hospital of
***LOCATION.1 and they informed him that they cannot provide it to him because it has been lost
because there have been changes; requested the supporting document of such
circumstance up to two times and finally they sent it to him.

SECOND: The Andalusian Health Service dependent on the Ministry of Health and
Families in writing of 03/05/2019 have indicated that the claimant requested their history
clinic to the Regional Hospital of ***LOCALIDAD.1 with a negative result and requested
information to the Hospital Management of the reasons it has informed that it had been
carried out an exhaustive search of the requested documentation; not even at the base
of data nor in the files of the Hospital are there any actions carried out on the claimant
prior to 2007 and that the documentation generated after said
date has been delivered to the claimant.

FOUNDATIONS OF LAW

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

control, and as established in art. 47 of the Organic Law 3/2018, of 5

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

Yo

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/10

hereinafter LOPDGDD), the Director of the Spanish Agency for Data Protection

is competent to resolve this procedure.

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

Public Administrations, in its article 64 "Agreement of initiation in the

procedures of a sanctioning nature", provides:

II

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the rules

regulators of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible

rating and sanctions that may apply, without prejudice to what

result of the instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that

attribute such competence, indicating the possibility that the presumed

responsible can voluntarily acknowledge their responsibility, with the

effects provided for in article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those that

may be adopted during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the

procedure and the deadlines for its exercise, as well as an indication that, in

If you do not make allegations within the stipulated period on the content of the

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the responsibility

imputed.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out in a phase

later by drawing up a List of Charges, which must be notified to

the interested".

In application of the previous precept and taking into account that no

formulated allegations to the initial agreement, it is appropriate to resolve the initiated procedure.

Article 58 of the RGPD, Powers, states:

III

"two. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

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

warning when the treatment operations have infringed the

provided in this Regulation;

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

Instead of the measures mentioned in this section, according to the

circumstances of each particular case;

(…)"

Article 32 of the RGPD "Security of treatment", establishes that:

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

nature, scope, context and purposes of the treatment, 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 measures and

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

which in your case includes, among others:

a) 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 evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to

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

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

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

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present 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 controller or the

manager and has access to personal data can only process said data

following the instructions of the person in charge, unless it is obliged to do so by virtue of the

Law of the Union or of the Member States".

IV

Law 41/2002, of November 14, regulating patient autonomy

and rights and obligations regarding information and clinical documentation, in

its article 17, dedicated entirely to the conservation of clinical documentation,

establishes in its first point that "Health centers have the obligation to

keep the clinical documentation in conditions that guarantee its correct

maintenance and security, although not necessarily on the original support, for the due assistance to the patient for the appropriate time in each case and, as minimum, five years counted from the date of discharge of each care process" and in its section 6 determines the following: "They are applicable to the clinical documentation the technical security measures established by the regulatory legislation of the conservation of files containing personal data and, in general, by Organic Law 15/1999, on the Protection of Personal Data".

Article 19 of the aforementioned Law 41/2002 indicates: "Rights related to the custody of medical records. The patient has the right that health centers establish an active and diligent custody mechanism for medical records.

This custody will allow the collection, integration, recovery and communication of the information subject to the principle of confidentiality in accordance with the provisions by article 16 of this Law".

The facts revealed in this claim are specified in the existence of a security breach in the systems of the claimed party allowing the vulnerability of the same when proving that the clinical history of the claimant with prior to the year 2007 they do not appear in the database or in the files of the Malaga General Hospital.

The RGPD defines violations of the security of personal data as "all those violations of security that cause the destruction, accidental or unlawful loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data".

From the documentation in the file, it is evident that the person claimed has violated article 32.1 of the RGPD, when there was a violation of the security of their systems by allowing the loss of clinical documentation related to the claimant.

The respondent himself in writing dated 08/02/2019 has indicated that the request for

documentation relating to the claimant's medical history was requested from the Hospital Regional Office of Malaga, and the Management of the aforementioned hospital reported the reasons for the claim stating that a search had been carried out of the documents requested by the interested party and that the result had been negative and that do not exist in the databases or in the files of the Hospital Regional Office of Malaga, any record of actions or attention given to the claimant before 2007.

It should be noted that currently the RGPD does not establish a list of the security measures that are applicable according to the data that are subject of treatment, but establishes that the person in charge and the person in charge of the treatment must apply the technical and organizational measures that are appropriate to the risk that the treatment entails, taking into account the state of the art, the costs of application, the nature, scope, context and purposes of the treatment, the risks of probability and seriousness for the rights and freedoms of the persons concerned.

In any case, when evaluating the adequacy of the level of security, particularly taking into account the risks presented by the processing of data, such as consequence of the accidental or unlawful destruction, loss or alteration of data data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data and that could cause damages physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the treatment from violating the

provided in this Regulation, the person in charge or the person in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as

encryption. These measures must guarantee an adequate level of security, including

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

The violation of article 32.1 of the RGPD is typified in the article

83.4.a) of the aforementioned RGPD in the following terms:

v

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

with 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:

the obligations of the person in charge and the person in charge in accordance with the

articles 8, 11, 25 to 39, 42 and 43.

a)

(…)

On the other hand, the LOPDGDD in its article 71, Violations, states that:

“The acts and behaviors referred to in the regulations constitute infractions.

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

And in its article 73, for the purposes of prescription, it qualifies as "Infringements

considered serious":

"Based on the provisions of 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:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance with

required by article 32.1 of Regulation (EU) 2016/679".

The facts revealed in this claim show the

vulnerability of the security measures implemented by the claimed party, causing

the loss of the claimant's medical records, which constitutes a violation of the

article 32.1 of the RGPD.

However, the LOPDGDD in its article 77, Regime applicable to

certain categories of controllers or processors, establishes the

Next:

SAW

"1. The regime established in this article will be applicable to treatments

of which they are responsible or entrusted:

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

institutions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

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

autonomous communities 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

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 Assemblies

Autonomous Legislative, as well as the political groups of the Corporations

Local.

2. When the managers or managers listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law, 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 on which it reports hierarchically, where appropriate, and those affected who have

the condition of interested party, if any.

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

data protection will also propose the initiation of disciplinary actions

when there is sufficient evidence to do so. In this case, the procedure and

sanctions to apply will be those established in the legislation on disciplinary regime

or sanction that results from application.

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

and the existence of technical reports or recommendations for treatment is proven

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 informed of the

resolutions that fall in relation to the measures and actions referred to

the previous sections.

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

analogous of the autonomous communities the actions carried out and the

resolutions issued under this article.

6. When the competent authority is the Spanish Agency for the Protection of

Data, it will publish on its website with due separation the resolutions

referred 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 would have committed the

infringement.

When the competence corresponds to a regional protection authority

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

its specific regulations.

In accordance with the available evidence and without prejudice to the

resulting from the investigation of the procedure, such conduct could constitute

principle on the part of the claimed the possible infringement of the provisions of article 32

of the GDPR.

However, the RGPD, without prejudice to the provisions of article 83,

contemplates in its article 77 the possibility of resorting to the sanction of warning

to correct the processing of personal data that is not in accordance with your

forecasts, when those responsible or in charge listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law.

In the case examined, it has been proven that the respondent does not have

Technical and organizational measures have been adopted to guarantee a level of security

capable of ensuring the confidentiality, integrity and availability of the

data avoiding its loss.

It is necessary to point out that not correcting said circumstances by adopting the

appropriate technical and organizational measures in accordance with the provisions of the

article 32.1 of the RGPD or reiterate the conduct revealed in the

claim and that is the cause of this procedure, as well as not informing

following this AEPD of the measures adopted could give rise to the exercise of

possible actions before the person in charge of the treatment so that they are applied

effectively the appropriate measures to guarantee and not compromise the

confidentiality of personal data and the right to privacy of

people.

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 ANDALUSIAN HEALTH SERVICE, with NIF Q9150013B, by

an infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the RGPD,

a warning sanction.

SECOND: REQUEST ANDALUSIAN HEALTH SERVICE, with NIF Q9150013B,

so that within a month from the notification of this resolution, prove: the

adoption of the necessary and pertinent security measures in accordance with the

regulations regarding the protection of personal data in order to prevent

incidents such as those that have given rise to the

claim correcting the effects of the infraction produced, adapting the aforementioned

measures to the requirements contemplated in article 32.1 of the RGPD.

SECOND: NOTIFY this resolution to the ANDALUZ HEALTH SERVICE,

with NIF Q9150013B.

THIRD

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

: COMMUNICATE this resolution to the Ombudsman,

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

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 period of month 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, the firm resolution may be provisionally suspended in administrative proceedings if the interested party expresses his intention to file a contentious appeal-administrative. If this is the case, the interested party must formally communicate this made by writing to the Spanish Agency for Data Protection, introducing him to the agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing of the contentious-administrative appeal. If the Agency were not aware of the filing of the contentious-administrative appeal within two months from the day following the notification of this resolution, it would end the precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es