 File No.: PS/00365/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter the claimant) on 06/18/2020 filed

claim before the Spanish Data Protection Agency. The claim is

directed against the CANTABRO HEALTH SERVICE with CIF S3933002B (hereinafter, the

SCS or the claimed one). The grounds on which the claim is based are that they have mixed

your health data and that of another person who has the same name and surname, but

different ID. He has informed the SCS on different occasions through

written to correct the error, with no success.

And provide the following documentation;

- Copy of email dated 11/16/2019 sent by ***EMAIL.1 and sent to

***EMAIL.2 where the name and surname of the claimant appear together with the email

tronic sender and the SCS stamp dated 11/25/2019. In that email

It is stated that your data has been mixed with that of another person who has your

name and surname the same as yours. That this problem detected it for the first time

in the year 2012.

- Copy of email dated 12/04/2019 sent by ***EMAIL.1 and sent to

***EMAIL.2 where the name and surname of the claimant appear together with the email

tronic sender and the SCS stamp dated 12/19/2019. In that email

it is stated that in the Health Center of ***LOCALIDAD.1 on date 11/29/2019,

after handing in his ID, the person who attended him saw on his screen that his data was not

the DNI corresponded with the authentic one, that the first numbers were the same and the last

scams and the lyrics were different.

- Copy of claim submitted on 01/10/2020 to the claimant.

Later, in July 2020, they informed him that the situation had been resolved; No

However, he called the Health Center of ***LOCALIDAD.1 in order to request an appointment

for the flu vaccine, since he has always been vaccinated there and they inform him that he had

to be vaccinated at the Santander Health Center where she was registered. That

after giving his DNI at the ***LOCALIDAD.1 Health Center, it was found that

There is no reference to his person nor does any information about him appear.

And provide a copy of the certificate from the SCS (Primary Care Management) dated and signed-

do to 07/01/2020, where it is stated that, after detecting the error, it has proceeded to

rectify the same with respect to the administrative data of the claimant. consists of

the certificate the name and two surnames of the claimant, as well as the third digits,

fourth, fifth, sixth of your ID as well as the letter.

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), with reference number E/05273/2020, transfer of di-

this claim to the respondent on June 26, 2020, to proceed to its analysis

sis and inform this Agency within a month of the actions carried out

to adapt to the requirements set forth in the data protection regulations.

THIRD: On 10/16/2020, the Director of the AEPD agrees to the admission to

limit of the claim.

FOURTH: In view of the facts denounced in the claim and the documents
data provided by the claimant, the Subdirectorate General for Data Inspection pro-
yielded to carry out preliminary investigation actions for the clarification
of the facts in question, by virtue of the powers of investigation granted to the
control authorities in article 57.1 of Regulation (EU) 2016/679 (Regulation
General Data Protection, hereinafter RGPD), and in accordance with the provisions
ed in Title VII, Chapter I, Second Section, of Organic Law 3/2018, of 5
December, of Protection of Personal Data and guarantee of digital rights (in
hereinafter LOPDGDD).

On 03/03/2021, a request for information is sent to the claimant. The notice-
tion is done electronically through notific@. The notice is delivered
dated 03/04/2021. No response received.

FIFTH: On 08/12/2021, the Director of the Spanish Agency for the Protection of
Data agreed to initiate a sanctioning procedure against the person claimed for the alleged infraction.
tion of articles 5.1.f) and 32.1 of the RGPD, sanctioned in accordance with the provisions of
Articles 83.5.a) and 83.4.a) of the aforementioned RGPD, considering that the sanction that may
would correspond would be a warning.

SIXTH: Once the initiation agreement was notified, the respondent submitted a written statement of allegations
on 08/23/2021 in which he states, in summary, the following: that he has no record
having received the documentation dated 06/26/2021; that at all times
tried to analyze and solve the facts and circumstances raised by the person
interested party, emphasizing the necessary security and confidentiality of their personal data.
sonal; that the interested person requested this SCS in exercise of his right of
rectification of personal data, having responded to it by resolution after
estimate and informing of the necessary preservation of your data in order to
adapt them to the health care that may be required; that have been adopted

precise measurements and facilitated communication with the person concerned at all times.

ment.

SEVENTH: On 10/13/2021 the period of practice tests began, according to

do the following:

Consider reproduced for evidentiary purposes the claim filed by the re-

claimant and its documentation, the documents obtained and generated that form

man part of the procedure E/08372/2020.

Consider reproduced for evidentiary purposes, the allegations to the initial agreement

of the referenced sanctioning procedure, presented by the defendant and the

accompanying documentation.

EIGHTH: On 11/16/2020, a Proposed Resolution was notified in the sense that

by the Director of the AEPD, the person claimed for infraction of the articles

5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the RGPD, with

warning.

After the period established by the claimant, at the time of this Resolution,

He had not submitted any brief of allegation.

NINTH: Of the actions carried out in this proceeding, they have been

accredited the following

PROVEN FACTS

FIRST. On 06/18/2020, the claimant filed a claim with the AEPD against the

claimed, stated that their health data and those of another person have been mixed

who has the same name and surnames, but different DNI and who made known

on different occasions through writings so that the error is corrected, the result

tado has been unsuccessful.

SECOND. The claimant has provided copies of the emails dated

11/16/2019 and 12/04/2019 addressed to the respondent; in the first he asks for protection

of your personal data that had been mixed with that of another person

with the same name and surnames, a situation that has dragged on since 2012 and, in the second

second, states that in the Health Center of ***LOCALIDAD.1 on date

11/29/2019, after handing in his ID, the person who attended him saw on his screen that in his data

The DNI did not correspond to the authentic one, that the first numbers were the same

and the last ones and the letter was different.

THIRD. The claimant provides a copy of the claim filed on the date

01/10/2020 due to the absence of responses to the emails sent and anomalies observed

vadas in relation to your data.

FOURTH. The affected party addressed a new written claim to the defendant on 06/16/2020

not having received any response to the letters sent previously as well

such as inattention and disinterest in their problem.

FIFTH. The complainant in writing dated 07/19/2021 has indicated that: “An error was detected

in the clinical documentation of a passive nature in the Care Management

Primary belonging to the claimant in relation to the clinical episode referred to the Cen-

Health Center of *** LOCATION.2 and that was registered in the clinical history

of Mrs. A.A.A., with DNI ***NIF.1 from the Health Center of ***LOCALIDAD.3 in Santan-

right”.

SIXTH. The respondent has provided clinical documentation of a passive nature

in the Primary Care Management belonging to the claimant, in her capacity as

MUFACE user who appears in the history of AP Cantabria, as well as Ms.

A.A.A., with DNI ***NIF.1, as a user of the Public Health Service of

the Community of Cantabria.

SEVENTH. The respondent has provided certification, dated 07/01/2020, of the Managing Director

representative of the Primary Care Management, responsible for data processing

relating to the health of all active and inactive users of the Autonomous Community

ma of Cantabria through the Corporate Viewer application of the Cantabrian Service of

Health, that he had proceeded to correct the error detected regarding the ad-

claims of the claimant, in her capacity as a user of MUFACE.

EIGHTH. The respondent has stated that the SCS Management Directorate

requested the rectification of personal data and administrative order of the fi-

active third person character in the C.S. Lardo and thus proceeded to merge with the fi-

file of the claimant's history. And it contributes written of the Coordinator of Systems of

Information from the GAP, which indicates:

The administrative data of the active record of Ms. A.A.A., with ID

***NIF.1, in ***LOCALIDAD.2 and thus it has proceeded to merge with the file of the history

co of the claimant.

In this way, the claimant's clinical history remains in the OMI history of

C.S. of ***LOCATION.2.

“06/26/2020

NINETH. It consists of an official letter from the Primary Care Management dated 07/01/2020 addressed to

addressed to the claimant, matter rectification of administrative personal data of users

ria Muface, in which it is pointed out:

"In relation to your request to proceed to make RECTIFICATION in data of

personal and administrative nature in the clinical documentation of a

passive and that works in the Primary Care Management, attached I send you certification

corresponding to the rectification operated according to prior verification by the Coordination-

ra of the Information Systems Service of this health institution. What is co-

notice for the corresponding purposes".

FOUNDATIONS OF LAW

Yo

II

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

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

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

to solve this procedure.

Article 5 of the RGPD establishes the principles that must govern the treatment

of personal data and mentions among them that of "integrity and confidentiality".

The cited article states that:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing

to and against accidental loss, destruction or damage, through the application of

appropriate technical or organizational measures ("integrity and confidentiality")".

(…)

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of digital rights

(hereinafter LOPDGDD), states that:

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

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

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

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

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

3. The obligations established in the previous sections will remain

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

of the treatment".

III

The documentation in the file offers clear indications that the

claimed, violated article 5 of the RGPD, principles related to treatment, in relation to

tion with article 5 of the LOPGDD, duty of confidentiality, when combining and mixing

the health data of the claimant with those of a third party with the same name and

llidos but different DNI.

The claimant considers that the combination of her health data with those of

a third person who has the same name and surnames, but a different DNI, and the

possibility that the data be known by their respective owners or third parties, sub-

puts a violation of the duty of confidentiality, contemplated in article 5.1.f)

of the RGPD, as well as of article 5 of the LO 3/2018, of December 5, of Protection

of personal data and guarantee of digital rights.

Article 5 of Organic Law 3/2018, of December 5, according to which: "the res-

responsible and in charge of data processing as well as all the people who in-

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

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

In turn, establishing article 5.1.f) of the aforementioned RGPD that: “Personal data

will be (...) f) treated in such a way as to guarantee adequate security

of personal data, including protection against unauthorized or unlawful processing

ci-to and against its loss, destruction or accidental damage, through the application of

appropriate technical or organizational measures ("integrity and confidentiality".

Duty of confidentiality or secrecy, which constitutes one of the manifestations

essentials of the fundamental right to protection of personal data (article 18.4

CE), and that in the present case it has been violated as manifested by the claim itself.

mado when he points out everything was due to human error, an error that enables access

not authorized to the data and that are known by third parties, as they are not identified as

correctly through your DNI: “An error was detected in the clinical documentation of a character

passive ter working in the Primary Care Management that belongs to the claimant

in relation to the clinical episode referred to the Health Center of ***LOCALIDAD.2 and that

was registered in the clinical history of Dª. A.A.A., with DNI ***NIF.1 of the

Health Center of ***LOCATION.3 in Santander”.

In addition, it has indicated that "The Managing Director of the Attention Management

Primary, responsible for processing data relating to the health of all

active and inactive users of the Autonomous Community of Cantabria through the

Corporate Viewer application of the Cantabrian Health Service, had proceeded to correct

correct the error detected regarding the administrative data of the claimant, in its

condition of user of MUFACE".

Article 83.5 a) of the RGPD, considers that the infringement of "the basic principles

costs for treatment, including the conditions for consent under the

articles 5, 6, 7 and 9" is punishable.

IV

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

"Infringements considered very serious:

1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

entail a substantial violation of the articles mentioned therein and, in particular,

ticular, the following:

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

established in article 5 of Regulation (EU) 2016/679.

(…)"

v

Second, it should be noted that the security of personal data

It is regulated in articles 32, 33 and 34 of the RGPD.

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 pro-

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

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

appropriate channels to guarantee a level of security appropriate to the risk, which in its

case include, among others:

a) pseudonymization and encryption of personal data;

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

permanent silence of treatment systems and services;

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

promptly 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

I lie.

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 a consequence

accidental or unlawful destruction, loss or alteration of personal data

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

torized to such 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

feel article.

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

warrant that any person acting under the authority of the person in charge or the person in charge

do and have access to personal data can only process said data following instructions

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.

The violation of article 32 of the RGPD is typified in the article

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

SAW

"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, alternatively,

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

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

greater amount:

a) the obligations of the person in charge and the person in charge pursuant to articles 8,

11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "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

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

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

(…)"

The facts revealed in this claim are specified in

non-compliance with the established technical and organizational measures violating the

confidentiality of the data by combining the health data of the claimant with the

of a third person with the same name and surnames, but different DNI.

7th

As far as security measures are concerned, the RGPD establishes in its

Article 5.1.f) as one of the principles in terms of data protection, that of treatment

storage of the data with adequate security, which means that they must apply

technical and organizational measures that are appropriate to protect against

unauthorized or unlawful treatment and the loss, destruction and accidental damage of the

data.

Article 32 of the RGPD establishes that technical and organizational measures must be applied

organization taking into account the state of the art, the costs of applying the

measures, 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 relation to the latter, the risks arising from

go from the processing of personal data: accidental destruction, loss or alteration

such or unlawful personal data, unauthorized communication or access to such data,

and that could cause physical, material or immaterial damages. (The Con-

Considering 83 of the RGPD is very enlightening in this regard).

These measures include: pseudonymization and encryption, the ability to

to ensure confidentiality, integrity, availability, and resiliency, the ability to

capacity to restore availability and access to data after an incident, process of

verification (not audit), evaluation and assessment of the effectiveness of the measures.

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

"(83) In order to maintain security and prevent the processing from violating the

established 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 with respect to

regarding the risks and the nature of the personal data to be protected. To the

assess the risk in relation to data security, should be taken into account

the risks arising from the processing of personal data, such as the destruction

accidental or unlawful loss, loss or alteration of transmitted personal data, conservation

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

data, susceptible in particular to cause physical, material or

immaterial".

In the present case, as evidenced by the facts and the documentation

that integrates the investigation file E/05273/2020, the AEPD transferred the claimant

do on 06/26/2020 the claim submitted for analysis requesting the contribution

of information related to the incident claimed and without stating the answer

of the claimed.

On this matter, the respondent points out that, in the event that the

documentation, it would have been processed like the other writings and communications

that are received, but not the letter of 06/26/2020, never received in said management.

However, the responsibility of the claimed party is determined by the incident

security dent revealed by the claimant, since it is responsible for

make decisions aimed at effectively implementing technical measures and

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

to ensure the confidentiality of the data, restoring its availability and preventing

access to them in the event of a physical or technical incident.

The documentation provided shows that the entity failed to comply with this obligation.

tion, due to the error made in the claimant's documentation when combining it

with that of a third party user equally of the health services at the time of its

unequivocal identification. As already indicated in the previous ground, the defendant

By means of a letter dated 07/19/2021, it indicated that: “An error was detected in the documentation

passive clinic operating in the Primary Care Management that belongs to

to the claimant in relation to the clinical episode referred to the Health Center of ***LOCA-

LIDAD.2 and that was registered in the clinical history of Mrs. A.A.A., with ID

***NIF.1 of the Health Center of ***LOCALITY.3 in Santander”.

However, as the respondent points out, "From the Management Department of the SCS,

requests the rectification of personal and order data…” and that “it had been

proceeded to correct the error detected regarding the administrative data of the re-

crying out, in her capacity as a user of MUFACE”.

Therefore, it is estimated that the defendant violated article 32 of the RGPD, infringing

tion typified in article 83.4.a).

viii

It should be noted that the LOPDGDD in its article 77, Regime applicable to de-

certain categories of data controllers or processors, establishes the following

following:

"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

tions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

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

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

d) Public bodies and public law entities linked to or de-

pending from 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 Legislative Assemblies

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

them.

2. When the persons in charge or persons in charge listed in section 1

had any of the infractions referred to in articles 72 to 74 of this law

organic, the data protection authority that is competent will issue resolutions

tion sanctioning them with a warning. The resolution will also establish

as the measures that should be adopted to stop the behavior or correct the effects

cough 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

gain of which it depends hierarchically, in his case, and to those affected who had the

Interested party status, if any.

3. Without prejudice to the provisions of the preceding section, the protection authority

tion of data will also propose the initiation of disciplinary actions when

there are sufficient indications for it. In this case, the procedure and the sanctions to

apply will be those established in the legislation on the disciplinary or sanctioning system.

dor 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 corresponding Official State or Autonomous Gazette.

gives.

4. The resolutions must be communicated to the data protection authority.

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

tions 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

ferred 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

tion.

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 evidence available to said conscientious conduct,

asserts, on the part of the defendant, the infringement of the provisions of articles 5.1.f) and 32.1-

of the GDPR.

The RGPD, without prejudice to the provisions of its article 83, contemplates in its article

Article 77 the possibility of resorting to the sanction of warning to correct the treatments

processing of personal data that do not conform to their expectations, when they are answered

officers or managers listed in section 1 committed any of the offenses

tions referred to in articles 72 to 74 of this organic law.

In the present case, the person claimed through the Management Department of the SCS

requested the rectification of personal data and administrative data of the

claimant, providing certification from the Primary Care Management, responsible

of the treatment of data related to the health of all active users and

inactive workers of the Autonomous Community of Cantabria in which he indicated that

proceeded to correct the error detected regarding the administrative data of

that, in its condition of user of MUFACE. There is also a letter addressed to the

claimant notifying him of the rectification carried out in the clinical documentation

passive in nature.

Lastly, he pointed out that in order to avoid incidents such as the one that gave rise to the

claim, alerts will be activated to health professionals who access the

clinical documentation of patients to review the exact identity of each

patient or user at the time of access, to avoid human error.

Therefore, it is not appropriate to urge the adoption of additional measures, having

taken reasonable measures, in accordance with the regulations on the subject of

data protection, which is the main purpose of the procedures regarding

those entities listed in article 77 of the LOPDGDD.

For all these reasons, in accordance with the applicable legislation and having assessed the criteria of

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the CANTABRO HEALTH SERVICE, with CIF Q3900738J, by

an infringement of articles 5.1.f) and 32.1 of the RGPD, typified in articles

83.5.a) and 83.4.g) of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to the CANTABRO HEALTH SERVICE,

with CIF Q3900738J.

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