 File No.: PS/00473/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

Of the actions carried out by the Spanish Data Protection Agency and in

based on the following

FACTS

FIRST: D.A.A.A. (hereinafter, the complaining party) dated 08/19/2020

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the MINISTRY OF HEALTH of the C.C.A.A. of

MADRID, with CIF S7800001E (hereinafter, the claimed party). The reasons in which

the claim is based on are as follows: the claimant states that a third party has

used his identity to change his affiliation to another Health Center and that

After filing police complaints, a new appointment has been given to the person who usurped his

identity.

And it provides:

- "List of pending appointments" document dated 08/05/2020 where

contains the name and surname of the claimant, in "date of birth" it contains

“11/26/1988” and there are two appointments in the month of August 2020.

- "List of health problems" document dated 08/05/2020 where

contains the name and surname of the claimant, in "date of birth" it contains

“11/26/1988”.

- "List of pending appointments" document dated 08/18/2020 where

There is an appointment for 08/10/2020 at the Health Center ***CENTRO.1.

- Police report.

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), said claim was transferred, within the scope of the

E/10590/2020, to the respondent on 10/08/2020, to proceed with its analysis and

inform this Agency within a month of the actions carried out to

comply with the requirements set forth in the data protection regulations.

The entity has not responded to the transfer of the claim.

THIRD: On 12/21/2020 the Director of the Spanish Protection Agency

Data agreed to admit the claim filed by the claimant for processing.

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

of previous investigative actions to clarify the facts,

having knowledge of the following extremes:

On 05/26/2021, a request for information is sent to the claimant. The

notification is made electronically through notific@. The notice consists

delivered on 05/27/2021. No response received.

FIFTH: On October 6, 2021, 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 32 of the RGPD and Article 5.1.d) of the RGPD,

typified in Article 83.4 of the RGPD.

SIXTH: On 10/06/2021, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the defendant, for the alleged infringement of articles 5.1.d) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the aforementioned RGPD.

SEVENTH: Once the initiation agreement has been notified, the person claimed by means of a written 10/14/2021 I request the correction of the initial agreement; correction that was notified by agreement of 10/26/2021.

On 11/15/2021, the respondent submitted a brief of allegations stating in summary: that there had been problems in the registry of the internet office, reason why which at the time could not have knowledge of the information requirement of the AEPD; that upon receipt of the initiation agreement, its correction was requested and that subsequently, he proceeded to respond immediately to the requests for information confirming that there had been no identity theft in the person of the claimant but a human error in the identification of two citizens with the same name and surname.

EIGHTH: On 11/18/2021 a period of practice tests began, remembering the following;

Consider reproduced for evidentiary purposes the claim filed by the claimant and his documentation, the documents obtained and generated by the Inspection Services that are part of file E/10590/2020.

Consider reproduced for evidentiary purposes, the allegations to the initial agreement PS/00473/2021 presented by the respondent and the documentation that they accompanies.

NINTH: On 02/14/2022 the requested Resolution Proposal was notified in the sense that the Director of the AEPD sanctioned the defendant for infraction of articles 5.1.d) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the GDPR, with warning.

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

He had not submitted any brief of allegation.

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

accredited the following:

PROVEN FACTS

FIRST. On 06/11/2020 it has entry in the Spanish Agency for the Protection of

Written data of the affected person stating that at the beginning of 2020 he requested for the first

turn your health card to the health center ***CENTRO.2, ; that dated 08/05/2020 to

request an appointment online with your doctor, you could only request an appointment for the health center

***CENTRO.1, C/ ***ADDRESS.1, Madrid; than calling the health center

***CENTER.2 checks that your DNI is correct but they also tell you that your

address is at C/ ***DIRIMIENTO.2 (Vallecas) and the telephone number is not the

yours; that someone has changed your data, although to carry it out you must comply

with a protocol: identify yourself and provide the registration certificate

updated, management that the health center ***CENTRO.1 seems to have omitted and has

caused another person to impersonate your identity; Although he has never used the

public health, there are reserved appointments and a medical history that does not correspond to him;

that has filed police complaints, although they have not taken any action or

have communicated with him.

SECOND. The claimant has provided a document List of pending appointments of the

Madrid Primary Health Care Service dated 08/05/2020, document

List of health problems dated 08/05/2020 and document List of appointments pending dated 08/18/2020 (where there is an appointment for 08/10/2020 in the Health Center ***CENTRO.1), relating to the third party whose name, surnames, coincide with the claimant.

THIRD. There is evidence provided Complaint before the National Police, dependencies of Madrid-Retreat on 08/06/2020.

FOURTH. The defendant in writing of 08/10/2021 has indicated that "the incidence produced has its origin in the fact that there is another citizen who coincides in name and surnames with the complainant, that is, there has been no impersonation of identity as such of the citizen, but because of a human error in the identification, by not following the established protocols, gave rise to confusion produced.

In this way, once the pertinent investigations have been carried out, it has been possible to conclude that, on the administrative record of the claimant, a change was made in the domicile of the same to have served the citizen with the same name and surnames, without having verified the applicant's DNI or passport.

FIFTH. The respondent has provided a report issued on 09/15/2021 by Management Primary Care Assistance in which the events that occurred and indicate the existing security measures and those adopted to prevent similar incidents occur.

SIXTH. There is a communication addressed to the citizen of 10/05/2021, where reported that, once the pertinent investigations had been carried out, in the month of September 2020 they proceeded to rectify ex officio those data of their history clinical and population information that were recorded by mistake.

FOUNDATIONS OF LAW

Yo

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

control authority, 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 solve this procedure.

II

The facts denounced are motivated by identity theft

of the claimant by a third party on the occasion of the change of their affiliation to another Center

of Health without a response to your claim.

In the first place, the RGPD deals in its article 5 with the principles that have

of governing the processing of personal data and mentions among them that of accuracy,

pointing out:

"1. The personal data will be:

(…)

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

reasonable for the personal data to be erased or rectified without delay

that are inaccurate with respect to the purposes for which they are processed

("accuracy");

(…)"

The foregoing must be put in relation to article 5, Accuracy of the

data, of the new Organic Law 3/2018, of December 5, on Data Protection

Personal and guarantee of digital rights (hereinafter LOPDGDD), which

states in section 1:

"1. In accordance with article 5.1.d) of Regulation (EU) 2016/679, the data will be

accurate and, if necessary, updated

(…)"

And Recital 71 of the RGPD provides that, "(...) in order to guarantee a

fair and transparent treatment with respect to the interested party, taking into account the

specific circumstances and context in which personal data is processed, the

data controller must use mathematical or statistical procedures

suitable for profiling, applying technical and organizational measures

measures to ensure, in particular, that factors that introduce

inaccuracies in personal data and the risk of error is minimized,

secure personal data in a way that takes into account possible risks

for the interests and rights of the interested party and prevent, among other things, effects

discrimination against natural persons for reasons of race or ethnic origin, opinions

politics, religion or belief, union membership, genetic condition, or health status

or sexual orientation, or treatment that gives rise to measures that produce such an effect".

III

The infraction that is attributed to the claimed one is typified in the

article 83.5 a) of the RGPD, which considers that the infringement of “the basic principles

for processing, including the conditions for consent under the

articles 5, 6, 7 and 9” is punishable, in accordance with section 5 of the aforementioned

Article 83 of the aforementioned Regulation.

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 72, it considers for prescription purposes, which are: "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

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

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

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

(…)".

IV

From the documentation in the file, it is evident that the person claimed

has violated article 5.1.d), principle of accuracy, in relation to article 5 of the

LOPGDD, Accuracy of the data, by confusing character data in its identification

of the claimant with those of a third party with the same name and surname without

have verified the DNI or passport as established by the protocol.

In relation to the aforementioned article and its updating (which would be the

of the principle of accuracy that could be understood as breached), requires that

“reasonable measures to eliminate or rectify without delay the data

data that are inaccurate with respect to the purposes for which they are processed”.

In other words, article 5.1.d) does not impose the adoption of disproportionate measures to

update the data, but the reasonable ones, taking into account the available means and the purpose

for which the data is used. This is also expressed in recital 39 of the RGPD.

In relation to this principle, in recital 39 of the GDPR, among other

issues indicates that "(...) to ensure that personal data is not kept

longer than necessary, the data controller must set deadlines for

its suppression or periodic review. All reasonable steps must be taken to

ensure that inaccurate personal data is rectified or deleted.

The claimant considers that a third person has used his identity to

change their affiliation to another Health Center and that a police report was filed

has given a new appointment to the person who usurped his identity, violating the principle of

accuracy that must govern the personal data, contemplated in the article

5.1.d) of the RGPD, as well as article 5.1 of LO 3/2018, of December 5, of

Protection of personal data and guarantee of digital rights.

Principle of accuracy, which is one of the essential manifestations

of the fundamental right of protection of personal data (article 18.4 CE), and that

in the present case, it has been violated as manifested by the defendant himself

when he points out that "It was found out that there is another patient who coincides in name and

surnames with the claimant…In this way, once the inquiries have been made

pertinent, it has been possible to conclude that, on the administrative file of the claimant,

made a change in the address of the same to have served the citizen with the

same name and surnames, without having verified the applicant's DNI or passport.

However, in its letter dated 10/08/2021, it states that “In turn, we must

reference that in compliance with the principle of accuracy contained in article 5 of the

GDPR, according to which the data processed must be accurate and, if necessary,

updated; by the person responsible for the treatment, all the

reasonable measures to promptly erase or rectify the data

that are inaccurate, and proactively, we have proceeded ex officio to

cancel from the claimant's medical record the records that did not correspond to his or her

person".

And that therefore "it is confirmed that there has been no impersonation

identity of the interested party, if not that the incident occurred is due to human error

in the identification of two citizens who have the same name and surname,

having detected the same, in a proactive way, the different

consequences that could have materialized.

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

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

v

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".

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

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

"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:

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:

(…)

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 GDPR defines personal data security breaches as "all

those breaches of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

otherwise, or unauthorized communication or access to such data".

SAW

From the documentation in the file, there are clear indications of

that the claimed party has violated article 32 of the RGPD, when an incident of

security as a result of the breach of the measures established to

avoid errors in the identification of users.

It should be noted that the RGPD in the aforementioned precept 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 apply technical and organizational measures that are appropriate to the risk involved the treatment, taking into account the state of the art, the application costs, the nature, scope, context and purposes of the treatment, the risks of probability and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate. to the detected risk, pointing out that the determination of the technical and organizational must be carried out taking into account: pseudonymization and encryption, capacity to guarantee confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (not audit), evaluation and assessment of the effectiveness of the measures.

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 provisions 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 ensure an adequate level of security, including the 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.

In this case, as evidenced by the facts and in the case file of investigation E/10590/2020 the AEPD transferred the claimed on 10/08/2020 the claim submitted for analysis and reporting to this Agency of the actions carried out to adapt to the requirements set forth in the data protection regulations.

The respondent has alleged in relation to what is indicated in the second antecedent of that no response had been given to the transfer of the claim presented, that everything has been due to problems in the registration of the internet office, which caused it to not could have earlier access to the requests sent by the Spanish Agency for Data Protection, which has meant that some notifications received are not have been able to respond in a timely manner.

However, the responsibility of the claimed party is determined by the bankruptcy of security revealed by the claimant, since it is responsible for taking

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 and prevent access to them in

case of physical or technical incident.

It seems evident that in the present case the measures established

to avoid errors in the identification of users as credited in the report

issued on 09/15/2021 by the Primary Care Assistance Management in which

describe the events that occurred, indicating that: “By sharing a name and surnames,

we understand that there has been a problem of unique identification of

citizens by managing both appointments and changes in the database

population dated 04/08/2020 and must be reinforced with the Health Centers

security actions involved in the processing of appointments for the

unique identification of citizens with the use of magnetic stripe readers

summons by means of the DNI or passport" and that "After the analysis carried out, it was concluded

that a change of address was made on the claimant's administrative file

from the CS ***CENTRO.1 when the “transient” citizen was attended to, to the

match your name and surname data, without having verified the unequivocal data of

ID card or passport".

Likewise, the respondent indicated in his letter of 10/08/2021: “Thus, it has been

produced a problem in the identification of the citizen to have managed so much

citations as the change in the population base without having applied the indications

prior to unequivocal identification...".

Therefore, it is estimated that the defendant is responsible for the violation of article

32 of the RGPD, infringement typified in its article 83.4.a).

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

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

7th

"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 the present case, the defendant has violated the regulations regarding protection of personal data both from the principle of data accuracy as well as their safety principle.

According to the available evidence, said conduct constitutes by the claimed party an infringement of the provisions of articles 5.1.d) and 32.1 of the GDPR.

It should be noted that the LOPDGDD contemplates in its article 77 the sanction of warning in relation to the processing of personal data that is not match your forecasts. In this regard, article 83.7 of the RGPD contemplates that "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 organizations public authorities established in that Member State.

Likewise, it is contemplated that the resolution issued may establish

measures to be taken to stop the behavior, correct the effects of the

infraction that had been committed and its adequacy to the requirements contemplated in

Articles 5.1.d) and 32 of the RGPD, as well as the provision of supporting means of the

compliance with what is required.

However, the respondent has acknowledged the mistake made, pointing out that

on the claimant's administrative record, a change was made in the address to

have served a citizen with the same name and surnames without having

checked the DNI or passport, which caused the violation of the principle of

accuracy and the breach of the security measures implemented for the

identification of users in domicile exchange operations, as well as for the

request for appointments, system provided by the respondent in the report issued on

09/15/2021 by the Primary Care Assistance Management.

Finally, it is indicated that although the measures indicated for the personnel that

performs these functions, they were already aware of them, since

Every fortnight the Espacio AP Madrid (regular information space

for Primary Care professionals), the next update will include

new review in the form of "Did you know that...", emphasizing the need for

observance of the established protocol. Also in the next training courses

will expressly affect the section on data protection and identification of

users.

Therefore, in light of the foregoing, it is considered that the response of the

claimed has been reasonable, correcting the incidence not proceeding to urge the

adoption of additional measures, having adopted measures of a technical and

organizations in accordance with the regulations on data protection for

prevent situations like the one that gave rise to this from happening again

claim, which is the main purpose of the procedures with respect to those

entities listed in article 77 of 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 MINISTRY of the COMMUNITY OF

MADRID. with CIF S7800001E, for an infraction of articles 32.1 and 5.1.d) of the

RGPD, typified in articles 83.4.a) and 83.5.a) of the RGPD, a sanction of

warning.

SECOND: NOTIFY this resolution to the MINISTRY OF HEALTH of the

MADRID'S COMMUNITY.

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

through the

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

Sea Spain Marti

Director of the Spanish Data Protection Agency

28001 – Madrid

www.aepd.es

sedeagpd.gob.es