Procedure No.: PS/00327/2019

 RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) on 02/13/2019 filed

claim before the Spanish Data Protection Agency. The claim is

directs against MINISTRY OF HEALTH AND SOCIAL POLICIES OF THE JUNTA

DE EXTREMADURA with NIF S0611001I (hereinafter, the claimed). The reasons in

that bases the claim are: the lack of security in access when requesting an appointment

advance for primary care consultations from their websites, since anyone

can easily access data from community health users and

manage them.

Attached screenshot web page and images.

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

Data Inspection proceeded to carry out the following actions:

On 04/01/2019, the claim filed for

analysis and communication to the claimant of the decision adopted in this regard. Equally,

he was required so that within a month he sent to the determined Agency

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 the same date, the claimant was informed of the receipt of the

claim and its transfer to the claimed entity.

The person claimed on 07/01/2019 alleged, in summary: That the Service

Health Extremeño (SES), in compliance with its purposes and with the aim of

facilitate the citizen's relations with the health administration I create a service of

health management of the citizen establishing two different levels: a level of

Appointment management in primary care and other clinical information management

related to specialized care.

This service called "online health center" allows access to the management

of appointments with your primary care center, limiting the information to date, time and

meeting place; likewise, the service allows the citizen to request an appointment,

modify or cancel it. For the management of the citizen's medical information, the

system requires complex authentication, reinforced with elements such as ID

electronic etc

That they are not in agreement with the vision presented by the claimant since if

it is true that for the dating area it is enough to enter date of birth

and DNI, the information that can be accessed is simply that related to the

Appointment in Primary Care, but in no case can access to another type of

information, such as medical history, treatments, health data or appointments of Care Specialized, for which a more complex authentication would be needed (DNI, electronic certificate, etc.).

However, the SES has assessed the modification of some aspects of security in relation to the claim received, pointing out, among others, the modification of the conditions of use and the prior acceptance of the conditions of use of the service.

THIRD: On 07/25/2019, 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 12/10/2019, the Director of the Spanish Protection Agency of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged infringement of article 5.1.f) of the RGPD, sanctioned in accordance with the provisions of the article 83.5.a) of the aforementioned RGPD.

FIFTH: Having been notified of the aforementioned initiation agreement, the respondent did not present a written allegations within the legal period established for it, so it is applicable what 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, for which a Resolution is issued.

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

PROVEN FACTS

FIRST: On 02/13/2019, the claimant submitted a written document in the AGPD, reasoned

due to the lack of security when requesting an appointment for primary care consultations

from its website, since anyone can easily access the data of

community health users and manage them.

SECOND: A copy of the claimant's DNI nº ***NIF.1 is provided

THIRD: The SES in writing of 05/17/2019 states "that the use of the service is

subject to rules of use, available from an accessible link once it has been

accessed, visible at the bottom of the web and can be consulted at the address

https://saludextremadura.ses.es/onilne/publico/infoLegal.xhtml", and that in the case of

unauthorized or consented access may occur, such as the case raised by the

claimant "it must be understood that there is no security breach in the

information system but, rather, the commission of a crime by someone who

access unauthorized data" and that it has assessed the modification of some aspects

security-related such as:

"- Modification of the conditions of use, adapting them to the prevention of

the commission of the crimes that have been referred to previously, with special

incidence on crimes related to the discovery and disclosure of

secrets

- Prior acceptance of the conditions of use of the service: although it is true that the use

of the CSOnline service is subject to conditions of use that have already been made

reference in this document and, as just indicated, will be modified in the

sense of the claim, it is proposed to include an express prior acceptance (opt in) of

the conditions of use. With this modification, the user declares to be aware of the

terms of use. With this modification, the user declares to be aware of the

conditions of use and, specifically, the possibility of committing a crime in

So to access data of third parties".

FOUNDATIONS OF LAW

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.

Yo

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 results

of 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

attributes such competence, indicating the possibility that the alleged perpetrator

can voluntarily acknowledge its responsibility, with the effects provided for in the

article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those

may adopt 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 the event

not to carry out

allegations within the stipulated period on the content of the agreement

of initiation, it may be considered a resolution proposal when it contains a

precise statement about the imputed responsibility.

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.

III

The facts denounced are specified in the absence of security measures

on the website designated by the SES to manage requests for prior appointments

primary care in health centers or services in Extremadura, since for

make an appointment it is only necessary to enter ID and date of birth, which would allow

access to other data linked to the patient by third parties violating the duty of

confidentiality.

Article 5, Principles related to the treatment, of the RGPD that establishes that:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing and

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

appropriate technical or organizational ("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".

IV

The documentation in the file shows that the SES violates the

article 5 of the RGPD, principles relating to treatment, in conjunction with article 5 of

the LOPGDD, duty of confidentiality, in relation to the website intended by the aforementioned

body in the management of requests for prior appointment of primary care in the

health centers in Extremadura, as is also justified by the fact that the

legal notice remembering that unauthorized access to data or information of third parties

it is a criminal act and an opt-in mechanism to accept the conditions,

understanding that before accessing or registering in the dating section

This duty of confidentiality, previously the duty of secrecy, must

understood that its purpose is to prevent leaks of data not

consented to by their owners.

Therefore, this duty of confidentiality is an obligation that falls not

only to the person in charge and in charge of the treatment but to everyone who intervenes in

any phase of the treatment and complementary to the duty of professional secrecy.

The respondent himself considers that although for the appointment it is enough to introduce

the DNI and date of birth, the information that could be accessed is the

related to the Primary Care appointment without being able to access another type of

information such as medical history, health data, etc., requiring authentication

more complex reinforced with other elements; however, it is no less true that

root of the claim has assessed the modification of some aspects related

with safety as the conditions of use, adapting them to the prevention

of the commission of the crimes and the prior express inclusion (opt in) of the conditions of

use, which would corroborate the weakness of the technical measures and

organizational measures implemented, the application of a modification of the

system access procedure.

v

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

basic for the treatment, including the conditions for the consent in accordance with

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

mentioned article 83 of the aforementioned GDPR, “with administrative fines of €20,000,000

maximum or, in the case of a company, an amount equivalent to 4% as

maximum of the overall annual total turnover of the previous financial year,

opting for the highest amount.

The LOPDGDD in its article 72, for the purposes of prescription, 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

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.

(…)”

However, the LOPDGDD in its article 77,

Regime applicable to

certain categories of controllers or processors, establishes the

Next:

IV

"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 case at hand, in this sanctioning procedure It is accredited that, in relation to the service established for the management of appointments of primary care centers, the regulations on Personal data protection.

According to the available evidence, said conduct constitutes by the defendant the infringement of the provisions of article 5.1.f) of the GDPR.

It should be noted that 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.

Likewise, it is contemplated that the resolution issued will establish the measures that it is appropriate to adopt so that the conduct ceases, the effects of the infraction are corrected

that had been committed, the adequacy of the treatment to the requirements contemplated

in article 5 of the RGPD, as well as the provision of accrediting means of the

compliance with what is required.

As indicated previously, it has been proven that the defendant

has not adopted pertinent measures that guarantee a level of security

capable of ensuring the confidentiality and integrity of the data, avoiding

unauthorized and unauthorized access, the built-in solution not being enough

by the claimed to reinforce the legal notice on its website to remember that the

unauthorized access to information is a crime, as well as the opt-in mechanism for

accept the conditions before accessing or registering in the dating section.

It is necessary to point out that if these deficiencies are not corrected by adopting

the appropriate measures in accordance with the provisions of article 5.1.f) of the RGPD in order to

ensure adequate security of personal data, including the protection

against unauthorized or unlawful processing and against loss, destruction or damage

accidental, through the application of appropriate technical or organizational measures or

or to reiterate the behavior revealed in the claim and that is the cause of the

this procedure, as well as not immediately informing this AEPD of the

measures adopted could give rise to the exercise of possible actions before the

responsible for the treatment in order to apply effectively the measures

appropriate to guarantee and not compromise the confidentiality of the data of

personal character and the right to privacy of individuals.

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 MINISTRY OF HEALTH AND SOCIAL POLICIES OF THE JUNTA DE EXTREMADURA (Extremadura Health Service), with NIF S0611001I, by an infringement of Article 5.1.f) of the RGPD, typified in Article 83.5 of the RGPD, a warning sanction.

SECOND: REQUIRE the MINISTRY OF HEALTH AND SOCIAL POLICIES OF THE BOARD OF EXTREMADURA (Extremadura Health Service), with NIF S0611001I, so that within a month from the notification of this resolution, proves: the adoption of the necessary and pertinent 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 infringement, adapting the aforementioned measures to the requirements contemplated in article 5.1.f) of the RGPD.

THIRD: NOTIFY this resolution to the MINISTRY OF HEALTH AND SOCIAL POLICIES OF THE GOVERNMENT OF EXTREMADURA (Extremeño Service of Health), with NIF S0611001I.

FOURTH

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

: COMMUNICATE

this resolution to the Ombudsman, of

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.

c/ Jorge Juan, 6

28001 – Madrid

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