 Procedure No.: PS/00250/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: The inspection actions are initiated by the receipt of a letter of

AAA claim (hereinafter, the claimant), in which it states that they have

caused improper access to his medical history by a worker of the

Extremadura Health Service (hereinafter SES), with professional category of

nurse. The accesses are made without the authorization of the claimant and without the mediation

a relationship that justifies it.

The complainant adds that the improper accesses are perfectly identified in

the Certificate of access to the clinical history, issued on 08/14/2020 by the Management of the

Badajoz Health Area of the Extremadura Health Service (SES) in response to the

official letter issued by the Court of Instruction No. 2 of Badajoz, in which there are 5

accesses produced between 10/02/2007 to 07/15/2019. Indicates that more accesses are missing

undue, which are pending obtaining by the Court.

Relevant documentation provided by the claimant:

-Cars issued by the Investigating Court No. 2 of Badajoz admitting for processing

complaint for revealing secrets and agreeing to practice evidence.

-Certificate of access to the clinical history held in the information system of the

Claimant's SES dated 08/14/2020.

SECOND: In view of the notified facts and the documents provided by the

SES, the Subdirectorate General for Data Inspection proceeded to carry out

preliminary investigative actions to clarify the facts described

in the previous sections, 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
established in Title VII, Chapter I, Second Section, of Organic Law 3/2018,
of December 5, Protection of Personal Data and guarantee of the rights
(hereinafter LOPDGDD), having knowledge of the following
ends:

BACKGROUND

Date on which the claimed events took place: July 15, 2019

Claim entry date: October 13, 2020

Complainant: A.A.A. (the claimant)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Claimed: EXTREME HEALTH SERVICE (SES)

INVESTIGATED ENTITIES

EXTREME HEALTH SERVICE, with NIF S0611001I, and with address at Avda. de
the Americas 2, 06800 Merida, Badajoz.

RESULT OF THE INVESTIGATION ACTIONS

On 11/12/2020, the claim was transferred to the SES within the framework of the
reference actions E/9118/2020. The transfer document was collected on the day
11/23/2020 according to your acknowledgment of receipt. After the granted period, on 02/10/2021
resolution is issued admitting the claim and urging the present actions of
inspection.

On 02/16/2021, information and documentation on the events was requested from the

SES, not having received a response as of the date of preparation of this report. The

The request was collected on 02/22/2021, according to acknowledgment of receipt. Attached to

request made the claim transfer document issued

above, indicating that there is no answer to it.

In the request made, the following information was requested from the SES:

1.- Copy of the report prepared and supporting documentation in relation to the

facts, which will contain the following aspects:

1–1. Detailed specification of the causes that have made the events possible.

1–2. Detailed description of the actions taken in order to minimize

adverse effects and for the final resolution of the incident, indicating the date and

time of the measures taken.

1-3. Measures taken to prevent similar incidents from occurring,

dates of implementation and controls carried out to verify its effectiveness.

2.- Regarding the security of the processing of personal data previously

to the facts:

2-1. Documentation accrediting the Risk Analysis that has led to the

implementation of security measures and copy of the Evaluations of

Impact, if any.

2-2. Detail those technical and organizational measures adopted to

guarantee a level of security appropriate to the risks detected with

in relation to the accesses by the health personnel to the clinical records of the

patients. Security policy adopted by the entity in relation to it.

However, on 04/05/2021 a reply was received from the SES to the transfer

carried out on 11/12/2020 within the framework of the reference actions E/09118/2020, in

the following terms:

"YO.

ABOUT THE BACKGROUND

The aforementioned letter requests this Public Administration to rule on

a claim received by the citizen -the claimant- on the 13th of

October 2020.

In said communication, it is requested:

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

The decision made regarding this claim.

In the event of exercising the rights regulated in articles 15 to

□

□

22 of the RGPD, accreditation of the response provided to the claimant.

□

the claim.

Report on the measures adopted to prevent the occurrence of

□

similar incidents, dates of implementation and controls carried out to

check its effectiveness.

Any other that you consider relevant.

□

In this sense, this document complies with said request,

providing in Annex 1 the communications with the claimant and, in the rest of the sections of this document, the information requested by the AEPD.

ABOUT THE ACCESS CONTROLS ALREADY ESTABLISHED IN THE

II.

EXTREME HEALTH SERVICE

The Extremadura Health Service (hereinafter, SES) is an autonomous organization of administrative nature, dependent on the Department of Health and Dependency of the Junta de Extremadura, which is entrusted with exercising the powers of administration and management of services, benefits and health programs that govern your operation by the national and regional regulations that apply to it.

In this sense, the Law of the Autonomous Community of Extremadura 3/2005, of 8 July, of health information and autonomy of the patient regulates in its article 35.3 the the patient's right to access and obtain copies or certificates of the documents that are part of your clinical history, such as "knowing in any case who has accessed your health data, the reason for access and the use that has been made of they". Well, regarding the exercise of this right, which has been requested by the claimant, it cannot be inferred from the documentation provided that there has been non-compliance on the part of this Administration because, in plain view, this information is in the hands of the complainant.

Translated this right to the information system that supports the clinical information of patients in the Extremadura Health Service, it should be noted that the execution Effectiveness of this right to know who and for what is accessing the Clinical History, translates into the necessary existence of a relationship that legitimizes the access of the health professional to a certain Clinical History. For this reason, when accessing the History of a patient currently being treated at the workplace

clinic (be it Hospitalization, Outpatient Consultations, Functional Tests, Hospital of

Day, Operating Room...), the computer system automatically understands that the reason

of access is Welfare, and this is reflected in said system. However, this is not a

automatic process, but the system only allows access to records of

patients who are either under active treatment or have an appointment on the agenda

of the professional or, well, they belong to the patients assigned to them in their quota.

When Medical History is accessed by searching for a patient (not

selecting it directly from a job list), the system forces you to choose a

access reason from among those configured for each profile. In this

In this sense, the following will appear to a specialist in Specialized Care:

The Patient Management reason is selected when access to the History

-

relates to an action to be performed on a patient that is not

is in the Clinical Workstation at that time, such as consultation or

review of documentation, preparation of reports, prior preparation of

consultation or surgical intervention, review of clinical orders and citations...

The Research Study motif is selected, as its own name

-

indicates, when access to medical history is related to work of

research in which that patient is included.

The DCL Request reason will be used when accessing the History is made

□

to respond to a Request for Clinical Documentation from the

patient or an authorized person.

The reason Occupational Incapacity is only available for profiles of

□

Inspection and they will select it when the access to the History is related to

a patient's work problem.

Access ONLY to the Patient Agenda is not a reason for access to the

□

Record; is the name with which access to the Agenda is identified

in the log of records of accesses to the Patient Agenda.

However, even if this access filter has been set, this does not imply that the

access is total, since each of the reasons that would legitimize access and that

just exposed does not imply unrestricted access to clinical information.

For this reason, each of the accesses is accompanied by access restrictions, since

that total access to health information would not make sense when the reason

justifies access is an administrative reason.

In this way, the public health regulations of Extremadura by which the SES is governed,

It is a regulation that offers greater rights to citizens with respect to their

clinical information; this with the recognition of the right to know who has

access to your health information. The exercise of this right, as well as the guarantee

of the confidentiality of the health information processed in the SES becomes effective

through access controls to clinical information.

Therefore, it can be inferred that the accesses to which the complainant refers occurred

fulfilling the requirements of legitimacy of access that emerge from the

obligations of the data protection regulations and those imposed by

internally from the Extremadura Health Service. Thus, in the SECOND Fact

used as an argument, the idea that, as pointed out, the

access was made taking advantage of her "professional category of nurse", since,

had the situations described in this section not occurred, access would not have been

possible. Therefore, the argument used that

produced an access “without mediating between them a care relationship of

nurse/patient” given that the system requests access to clinical information

the existence of a reason that legitimizes access.

Likewise, the arguments described in Fact

THIRD, where the accesses made by Mrs. B.B.B. are noted, since

all accesses to the information should have been, and were, motivated by one of the

the previously foreseen and detailed scenarios.

ABOUT THE FORUM

III.

This part does not seek to question the authority of the AEPD, nor the information

provided by the complainant; however, the SES in its responsibility does not consider

opportune to deal with complaints or requests that do not start from a solid base. In this

sense, the FIRST Fact of the brief presented by the complainant refers

to facts that, well, should be understood as subjective or, at least, hardly

objective, such as the exercise of "strict control over life and person"

that did not allow the complainant "to lead a normal life and rebuild his life

sentimental".

As it is not objective information, the SES considers that it should not rule on this sense and that, rather, corresponds to another area, specifically to the organs judicial, establish whether the facts are as reported. understand, then, that there is a spirit of this Administration to collaborate, as long as it is possible, but it is understood that the facts denounced have to do with actions or omissions typified in the Penal Code on which the SES cannot do nothing more than collaborate with the judicial bodies that decide them.

Defined the legitimacy of access to a patient's information (the complainant) by a worker of the public health system (the defendant), given that without the existence of said legitimacy, access would be technically impossible, the SES understands that the reported situation must wait until it has the status of Proven Fact (understood as the account of events subject to prosecution that the judicial body has considered true). This is because it is also understood that the facts denounced do not correspond to a breach of the regulations of data protection of the SES as Responsible for the Treatment if not, rather as a crime (which could well be classed as revealing secrets) committed by a person, yes, a worker of the SES, in a private sphere in which the SES as an employer it has no scope.

Yes, mediating a sentence that establishes the reported facts as facts tested, having the SES knowledge of them, the measures will be taken timely internal measures based on the Internal Regime as described in the legal notices of the logins of the users of the information system.

Until that moment, the SES understands that this procedure must be filed and, in the event of a ruling favorable to the accused, notify the SES so that that the corresponding internal sanctions be established.

ON THE COMPLIANCE WITH THE OBLIGATIONS OF THE SES AS

IV.

RESPONSIBLE FOR THE TREATMENT

On the other hand, regarding the obligations of the Extremadura Health Service, such as

responsible for the treatment, and in coordination with what is stated at the beginning of the

Second allegation (II), the SES has been fulfilling its obligations as

responsible for the Treatment regarding the requests made by the complainant. I know

pointed out in the aforementioned allegation the existence, as a result of the legislative development of Extremadura

of a right to “know who accesses clinical information” and, view the information

provided by the complainant, it is understood that the SES has complied with said

obligations.

A different question is, if the denouncer understands that the person denounced has

breached its confidentiality obligations and, if so, once it is shown

as a proven fact, you can go to the SES so that the necessary measures can be taken.

timely.

ON THE MEASURES ALREADY APPLIED BY THE SES

v.

Prior to becoming aware of the complaint being forwarded, the SES, in the field of

its proactive responsibility had already taken measures that guarantee the

confidentiality of information.

(1)

Access control: access to clinical information of patients in the

Extremeño Health Service is only given when the control standards of

access;

a.

Firstly, information access control is segregated into

function of the professional role of the information system, that is, only those

who, due to their functions and obligations, must have access to clinical information

and, within these, depending on the purpose, you have access to all or part of said information.

information.

b.

Being legitimized to access clinical information by the professional role, the

access to citizens' data is not free for users, having to mediate

a relationship that legitimizes access to specific data, namely, being part of the

"quota" of the health professional, having him quoted on the agenda or being in a

active treatment. If these circumstances do not occur, access is not possible.

c.

Granted, where appropriate, access having given the two circumstances

above, this is not necessarily full access or access to History

Complete clinic since the accesses are defined for specific purposes and

these, in turn, have defined what information they give access to based on said purpose.

We speak, therefore, of a double legitimation based on (1) the professional role and (2) the

purpose of access and, added to the need for the existence of a reason that

legitimize access.

(two)

Legal notice at the beginning of the session in which users are reminded that the
information that is accessed is confidential and should only be treated with the
purpose that legitimizes access.

Uses other than the above purposes are considered inappropriate and could
considered labor misconduct or, where appropriate, a crime and lead to the initiation of proceedings
in the corresponding legal field.

“[…] It is contrary to good faith to attempt to access information for which there is no
has permissions or privileges or that is not directly related to their
functions, as well as filtration of any type of data, especially of character
personal, outside the corporate network.

In this sense, the user of the computer system […] knows the responsibilities
established in the Criminal Code, in the Data Protection regulations and in the rest
Spanish legislation on illicit use, contrary to morality, good faith and the
customs of computer tools, without prejudice to the responsibility
derived from the applicable internal regulations.

In order to guarantee compliance with the security policy, the SES may
monitor communications and/or files received/sent by users via
through the resources and systems of the entity in the event that there are suspicions
founded that resources are being misused. […]”

The acceptance of this legal notice is mandatory to be able to access the system of
information.

(3) Training pills, reminders, circulars... regarding the duties of secrecy
and confidentiality, security advice and the like that, from the Subdirectorate of

Information Systems together with the figure of the Data Protection Delegate

launched to all users of the system, as well as other resources accessible from the

"SES portal" to which all users of the information system have access

of the SES.

THIRD: On May 26, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, for the

alleged infringement of Article 32 of the RGPD, Article 5.1.f) of the RGPD, typified in the

Article 83.5 of the RGPD.

FOURTH: Once the agreement to initiate this sanctioning procedure has been notified, the

SES, as the person in charge, has not presented arguments.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It is proven that a third party other than the claimant agreed

unduly to his clinical history in the SES, on several occasions without

the SES intervened to prevent it once the incident was known.

SECOND: The cause that caused the improper access was the lack of measures

technical and organizational systems implemented in the information and control system of

SES accesses.

THIRD PARTY: It is stated that an alien third party had knowledge of the data of the

claimant in the clinical history of the SES categorized as special

according to art. 9 of the GDPR.

FOUNDATIONS OF LAW

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

control, 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

resolve this procedure.

Yo

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

II

“Article 5 Principles relating to the treatment

1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational structures (“integrity and confidentiality”).”

In the present case, it is proven that the personal data of the claimant

relating to his medical history that appear in the SES information system were

improperly accessed by a third party, violating the principles of

integrity and confidentiality, both established in the aforementioned article 5.1.f) of the RGPD.

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

III

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

of the 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 (The underlining is from the AEPD).

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

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

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

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

physical, material or non-material damages, particularly in cases where

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

identity or fraud, financial loss, reputational damage, loss of

confidentiality of data subject to professional secrecy, unauthorized reversal of the pseudonymization or any other significant economic or social damage; in the cases in which the interested parties are deprived of their rights and freedoms or are prevent exercising control over your personal data; In cases where the data treated personalities reveal ethnic or racial origin, political opinions, religion or philosophical beliefs, militancy in trade unions and the processing of genetic data, data relating to health or data on sex life, or convictions and offenses criminal or related security measures; In cases where they are evaluated personal aspects, in particular the analysis or prediction of aspects related to the performance at work, economic situation, health, preferences or interests personal, reliability or behavior, situation or movements, in order to create or use personal profiles; in the cases in which personal data of vulnerable people, in particular children; or in cases where the treatment involves a large amount of personal data and affects a large number of interested."

In the present case, of the investigation actions carried out, the selection of the reason for accessing the clinical history of a SAS patient is not verified with the access profile of the user, leaving, consequently, access to the information to the discretion of the accessing user.

Therefore, as a consequence of the lack of implementation of technical measures and adequate organizational rules that are mandatory for Public Administrations as indicated in RD 3/2010, which regulates the National Scheme of Security (ENS), has caused access by a third party outside the data housed in the clinical records information system of the SES. It does not contain the performance of the mandatory risk analysis and, where appropriate, impact assessment act on the treatment of health data of SAS patients. It is also not stated that

the SAS has implemented a process of verification, evaluation and continuous assessment

IV

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

The actions carried out show the absence of security measures both technical and organizational, with which the SES had carries out treatment operations in relation to the health data of the records clinical. Nor is there evidence of the adequacy of the processing operations of the SES to the National Security Scheme at the time of improper access.

The consequence of this implementation of deficient security measures was the Exposure to a third party outside of personal data relating to the health of the claimant. That is, the affected party has been deprived of control over their data information related to your medical history.

It should be added that, in relation to the category of data to which the third person outside has had access, they are in the category of special according to what provided in art. 9 of the RGPD, a circumstance that supposes an added risk that must assess in the risk management study and that increases the degree requirement of protection in relation to the security and safeguarding of the integrity and confidentiality of these data.

This risk must be taken into account by the data controller, who must establish the necessary technical and organizational measures to prevent the loss of

control of the data by the data controller and, therefore, by the data controllers.

holders of the data that provided them.

Article 83.4.a) of the RGPD, states the following:

(…)

v

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

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 in accordance with articles 8, 11,

25 to 39, 42 and 43".

Article 83.5.a) of the RGPD, states the following:

(…)

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

paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or,

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

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

the largest amount:

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

consent under articles 5, 6, 7 and 9";

Article 76 of the LOPDGDD under the heading "Sanctions and corrective measures",

points out the following:

1.

The penalties provided for in sections 4, 5 and 6 of article 83 of the

Regulation (EU) 2016/679 will be applied taking into account the criteria of

graduation established in section 2 of the aforementioned article.

1.

It will be possible, complementary or alternatively, the adoption, when

appropriate, of the remaining corrective measures referred to in article 83.2

of Regulation (EU) 2016/679.

Article 71 of the LOPDGDD establishes, under the heading "Infractions" the following:

The acts and behaviors referred to in sections 4, 5 constitute infractions.

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

contrary to this organic law.

SAW

It establishes article 72.1.a) of the LOPDGDD, under the heading "Infringements

considered very serious", the following:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

considered very serious and will prescribe after three years the infractions that suppose

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

following:

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

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

In the present case, the infringing circumstances provided for in article

72.1.a) of the LOPDGDD transcribed above.

It establishes article 73 of the LOPDGDD, under the heading "Infringements considered

serious” the following:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679,

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

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

following:

f) The lack of adoption of those technical and organizational measures that result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679.

In the present case, the infringing circumstances provided for in article 73 concur.

section f) of the LOPDGDD transcribed above.

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

Chapter III on the "Principles of the power to impose penalties", in article 28

under the heading “Responsibility”, the following:

"1. They may only be sanctioned for acts constituting an administrative infraction.

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

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

independent or autonomous estates, which are responsible for them

title of fraud or guilt”

Lack of diligence in implementing appropriate security measures

with the consequence of breaching the principle of confidentiality, constitutes the

element of guilt.

viii

Article 58.2 of the RGPD, states the following:

2. Each supervisory authority will have all of the following corrective powers

listed below:

(…)

b) send a warning to any person responsible or in charge of the treatment when the

treatment operations have violated the provisions of this Regulation;

For its part, the Spanish legal system has chosen not to penalize

imposition of an administrative fine on public entities, such as the SES, such as

It is indicated in article 77.1. c) and sections 2, 4, 5 and 6 of the LOPDDGG:

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

who are responsible or in charge:

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

autonomous and the entities that make up the Local Administration.

2. When those responsible or in charge listed in section 1 committed

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

organic, the data protection authority that is competent will issue a resolution

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

measures to be taken to stop the conduct or correct the effects of the

offense that had been committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the body of the

that depends hierarchically, where appropriate, and to those affected who had the condition

interested party, if any.

4. The data protection authority must be notified of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

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

of the autonomous communities the actions carried out and the resolutions issued

under this article.

6. When the competent authority is the Spanish Data Protection Agency,

this will publish on its website with due separation the resolutions referring to

the entities of section 1 of this article, with express indication of the identity of the

responsible or in charge of the treatment that had committed the infraction.>>

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Agency for Data Protection, RESOLVES:

FIRST: IMPOSE EXTREME HEALTH SERVICE, with NIF S0611001I,

for the infringement of Article 32 of the RGPD typified in Article 83.4.a) of the RGPD the

sanction of WARNING, and for the infringement of article 5.1.f) of the RGPD,

typified in Article 83.5.a) of the RGPD, the sanction of WARNING.

SECOND: NOTIFY this resolution to the EXTREME DEPARTMENT SERVICE

HEALTH.

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, 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 month from counting 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, may provisionally suspend the firm resolution in administrative proceedings if the The interested party expresses his intention to file a contentious-administrative appeal. If this is the case, the interested party must formally communicate this fact by writing addressed to the Spanish Agency for Data Protection, presenting it through Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

C/ Jorge Juan, 6

28001 – Madrid

938-131120

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es