 Procedure No.: PS/00384/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Mr. A.A.A., on behalf of Mr. B.B.B. (hereinafter, the

claimant) on 07/30/2019 filed a claim with the Spanish Agency for

Data Protection. The claim is directed against the GENERAL DIRECTORATE OF THE

CIVIL GUARD with NIF S2816003D (hereinafter, the claimed). The reasons in which

bases the claim are, in short: the assignment without consent and the dissemination of

personal information of the affected party contained in the agreement to initiate the suspension of

your weapons license, when said document is attached in an email

sent on 09/17/2018 from the generic account, al-cmd-almeria-ia@guardiacivil.org,

ownership of the Arms Intervention Unit of the Civil Guard of Almería, to the

generic account al-pto-canjayar@guardiacivil.es, owned by the Unit of the Post of

Canjayar, in order for the interested party to be notified.

After the resolution of inadmissibility for processing, dated 09/06/2019, the claimant

files an appeal for reversal alleging that the email was sent in the

scope of work to generic recipients with sensitive personal data. that the

sender and recipient email accounts are not personal but accounts

of certain departments of the Civil Guard, being able to be consulted by

indeterminate and numerous people who are part of them.

On 10/16/2019, an approving resolution is issued.

SECOND: In view of the facts denounced in the claim and the

documents provided by the claimant, the Subdirectorate General for Inspection of

Data proceeded to carry out preliminary investigation actions for the

clarification of the facts in question, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the Law

Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of

digital rights (hereinafter LOPDGDD).

On 12/04/2019, the respondent sends this Agency the following information:

1. That what is called in the complaint a generic email account

it is not such That the CIVIL GUARD has an isolated private communication network

from abroad and which can only be accessed through official means within which

there is a messaging system called GroupWise in which each Unit or

Work Station may be assigned an address for exclusive use by the

staff of that Unit for internal communications and which is accessed after

identify yourself with a smart card and an individual password.

2. That this system is used on a regular basis for communications between the

different Units, as it is guaranteed that any communication or

documentation that is sent through it is isolated from the outside and

maintains your level of confidentiality.

3. Show your disagreement in relation to the indiscriminate transfer of data

personal. It points out that the instruction of an administrative procedure requires that

between the different bodies or departments involved in it, to share

information for the sake of being able to carry out the function assigned to the Administration (the

control of the documentation that authorizes the possession of small arms to guarantee

proper use of the same and by derivation the safety of third parties) and the right

of the company to know the facts on which such action is based and receive

complete information about it.

4. That the complainant himself was one of those who accessed said system of

courier on the date of remittance of the same together with the Sergeant commander of

post and four other civil guards. That the fact of having access to the

messaging does not imply that such an act was carried out.

5. That if after more than a year has elapsed since said communication the

complainant does not indicate that it has had transcendence and with it a damage

for him, presumably the one who agreed to it was him or those in charge of

notify you of the initiation of the procedure.

6. That regarding the Intervention of Weapons sender, access to said system of

messaging was within the reach of the personnel assigned to said unit, a total of eleven

people, which, as in the previous case, does not mean that they accessed

said document.

THIRD: On 11/08/2020, the Director of the Spanish Protection Agency

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

infringement of articles 5.1.f) and 32.1 of the RGPD, sanctioned in accordance with the

provided in article 58.2.b) of the RGPD.

FOURTH: Notified of the initiation agreement, the respondent on 11/30/2020 submitted a written

of allegations pointing out that it was reiterated in the allegations made the

05/30/2020 and that the claimant's complaint refers to a mere possibility that

someone had accessed your personal data without you being able to say so, so

the alleged infractions have not materialized.

FIFTH: On 12/14/2020 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/10062/2019.

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

filed by the defendant

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/12

- Ask the claimant for a copy of the documentation in their possession regarding the

sanctioning procedure that for any reason had not been provided in the

time of the claim or, if it deems it appropriate, any other manifestation in

relation to the alleged facts.

SIXTH: On 05/27/2021, a resolution proposal was formulated in the sense

Next:

1. That the Director of the Spanish Agency for Data Protection addresses

warning against the defendant, for the infringement of articles 5.1.f) and 32 of the

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

Regulation.

2. That the respondent be required so that, within the period determined, adopt the

necessary measures to adapt the treatment operations carried out to the

personal data protection regulations, with the scope expressed in the

Fundamentals of Rights of the proposed resolution.

SEVENTH: Notification to the claimed entity of the aforementioned resolution proposal, with date 06/07/2021, this Agency received a letter of allegations in which states again that it has not been proven that a third party had knowledge of the personal data, nor the damage caused to the claimant.

On the other hand, in relation to the transfer of information from one managing body to another, Actions have been put in place to avoid future repetitions, such as the Circular prepared by the Data Protection Delegate (DPD), indicated with the number DPD 1-2020, of 12/01/2020, which has been disseminated to all Units and will be is available on the DPD intranet.

Provide a copy of this Circular, in which the following is stated:

“Regarding the first question, guarantee confidentiality, provided that it is attached to a electronic communication documentation that includes personal data, especially when the they contain health data (medical, psychological or health documentation of any Type); related to criminal or administrative sanctions (sentences, notification of sanctions, disciplinary proceedings); or referring to actions derived from the foregoing (withdrawal of weapons, citations to appear, etc.), must be sent in encrypted folders with password that will be provided prior identification of the applicant as belonging to the Recipient Unit or Body as the one that must resolve the issue, and should not be provided to intermediary units or bodies that do not need to know the specific content of the documentation for its processing, limiting to the maximum the number of people who access it and must be able, if necessary, to respond to a complaint to identify those who have accessed it.

In those cases in which it is documentation that must be delivered to the interested, it will be ensured that said delivery is made guaranteeing the maximum possible reserve and that this be carried out by their direct command, avoiding that it be carried out by personnel who

performs bureaucratic tasks, unless said delivery materializes in a sealed envelope; in

In these cases, it must be stated on the receipt that the receiver receives the documentation with

such guarantees of confidentiality.

When it comes to documents that must be signed by the interested party and returned to the

sending unit or body, what is stated in the previous paragraph will be observed for the delivery and

signature; and the aforementioned measures will be adopted for their return through

electronic communications.

In those cases in which other means of communication, postal, etc., are used,

adopt analogous measures adapted to the environment, always with the aim of guaranteeing the

confidentiality of personal data.

Improper practices such as printing and keeping a copy of the documentation must be avoided.

forwarded or delivered, which compromise and make it difficult to maintain the confidentiality of said information.

information over time.

Of the actions carried out in this proceeding, there have been

accredited the following:

PROVEN FACTS

FIRST: Dated 09/17/2018, from the email address al-cmd-

almeria-ia@guardiacivil.org, assigned to the Arms Intervention Unit of the

Guardia Civil de Almería, an email was sent to the address al-pt-

canjayar@guardiacivil.es, belonging to the Canjayar Post Unit, with the

matter “Rev. Agreement to start the suspension of a weapons license type... (type of license, name,

surnames and DNI of the claimant) for notification to the interested party".

The text of the message is as follows:

"Notification is sent for its delivery to the interested party, and a copy dated and

signed from its reception to this I.A., for its remission to the Zone Headquarters, as

is indicated in the e.c. attached".

This email attached the document to which your subject refers, which corresponds to

agreement to initiate the procedure for the suspension of the weapons license initiated at the

claimant by the General Directorate of the Civil Guard. In this document there are

the identification data of the claimant, his administrative situation and destination, as well as

all the factual circumstances that determined the initiation of said

procedure (police and judicial actions followed against the claimant for

gender violence).

SECOND: The respondent has informed this Agency that it has a system of

courier that assigns to each unit or position an address for exclusive use by the

staff of the unit in question. In the case of the email address

corresponding to the Canjayar Post Unit, it is indicated that it could be

accessed by the Sergeant Commander of the post, the claimant and four guards

more civilians.

FOUNDATIONS OF LAW

Yo

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.

Article 58 of the RGPD, Powers, states:

II

"two. Each control authority will have all the following corrective powers indicated below: continuation:

(…)

b) sanction any person responsible or in charge of the treatment with a warning when the treatment operations have violated the provisions of this Regulation;

(…)".

In the first place, 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":

"1. The personal data will be:

(…)

f) processed in such a way as to ensure adequate security of personal data, including protection against unauthorized or unlawful processing and against loss, accidental destruction or damage, through the application of technical or organizational measures appropriate ("integrity and confidentiality").

(…)".

Article 5, Duty of confidentiality, of the LOPDGDD, states that:

"1. Those responsible and in charge of data processing as well as all the people who intervene in any phase of this will be subject to the duty of confidentiality to which refers to article 5.1.f) of Regulation (EU) 2016/679.

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

of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even when

the relationship of the obligor with the person responsible or in charge of the treatment had ended.

III

The documentation in the file proves that the defendant violated the

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

the LOPGDD, duty of confidentiality, materialized in the dissemination of data of

personal nature relating to the claimant contained in the initiation agreement

suspension of his gun license, attached to an email that was

sent to the generic account al-pto-canjayar@guardiacivil.es, which is owned by the

Unit of the Post of Canjayar (Almería), which was within reach and could be

accessed by the staff assigned to said unit, a total of five people,

in addition to the claimant.

This duty of confidentiality, previously the duty of secrecy, is intended to

prevent leaks of data not consented to by the holders of the data.

themselves.

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

responsible and in charge of the treatment but to anyone who intervenes in any

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

The respondent has argued that there is no indiscriminate transfer of data

and that the instruction of an administrative procedure requires that

different administrative units or departments share information. Without

However, what happens in this case does not fit this scheme, because the

information regarding the complainant is not forwarded to a unit that intervenes

formally in the proceeding against it.

Likewise, the respondent has stated that the proceedings do not prove that a

third party has accessed confidential information relating to the complainant. Nevertheless,

does not take into account the factual circumstances that have given rise to this

process. In this case, it is clear that the notification of the agreement to start opening

of a weapons license suspension procedure, followed against the

claimant, was sent to a generic email account, owned by the

Unit of the Canjayar Post, in order to be delivered to the interested party,

that is, to the claimant. This shipment, in itself considered, already supposes an infraction

to the personal data protection regulations, to the extent that it enables the

access to information relating to the claimant by third parties. Besides, the

formalization or completion of this procedure, with the delivery of the agreement to the

claimant, implies that a third party or several accessed the information. To this

In this regard, it is advisable to reproduce again the instructions contained in the

mentioned email about the delivery of the documentation:

“Notification is sent for its delivery to the interested party, and a copy dated and

signed from its reception to this I.A., for its remission to the Zone Headquarters, as

is indicated in the e.c. attached".

IV

Article 83.5 a) of the RGPD, 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 RGPD, “with administrative fines of €20,000,000 as

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.

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 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 the

Article 5 of Regulation (EU) 2016/679.

(…)”.

v

Second, 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, the

scope, context and purposes of the treatment, as well as risks of probability and severity

variables for the rights and freedoms of natural persons, the person in charge and the person in charge

of the treatment will apply appropriate technical and organizational measures to guarantee a level

appropriate to the risk, which, where appropriate, includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

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

fast in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of the effectiveness of the measures

technical and organizational to guarantee the security of the treatment.

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

risks presented by the processing of data, in particular as a consequence of the

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

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

data.

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

certification approved under article 42 may serve as an element to demonstrate the

compliance with the requirements established in section 1 of this 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 processor and having 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 article 83.4.a)

of the aforementioned RGPD in the following terms:

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

section 2, with administrative fines of a maximum of EUR 10,000,000 or, in the case of a

company, of an amount equivalent to a maximum of 2% of the total annual turnover

of the previous financial year, opting for the highest 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 71, Violations, states that:

“The acts and behaviors referred to in sections 4, 5 and 6 of the Law constitute infractions.

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to this

organic Law".

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

serious”:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679, they 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 breach, as a consequence of the lack of due diligence, of the measures

technical and organizational that had been implemented in accordance with the requirements of article 32.1

of Regulation (EU) 2016/679.

(…)”.

SAW

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”.

From the documentation in the file, it is proven that the respondent has

violated article 32.1 of the RGPD, when a security incident occurred

consisting of transferring the claimant's data through a corporate email

that was accessible to all members of the recipient unit.

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 technical measures 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 of the 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 technique and cost of its application with respect to the risks and the nature of the data personal to be protected. When assessing the risk in relation to the safety of the data, the risks arising from the processing of the data must be taken into account such as accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data, susceptible in particular to cause physical, material or immaterial".

In the present case, as evidenced by the facts and in the framework of the file of investigation E/10062/2019, the claim filed was transferred to the defendant for analysis, requesting the provision of information related to the incident claimed in which it shows its disagreement with the indiscriminate transfer of data, although it states that access to the internal messaging system was within the reach of the staff assigned to that unit.

The liability of the claimed party is determined by the security breach disclosed by the claimant. The respondent 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, among them, those aimed at restoring the availability and access to data quickly in the event of a physical incident or technical. However, from the documentation provided prior to the processing of the procedure, it is not known whether any steps had been taken to put

end to incidents such as the one that gave rise to the claim.

In accordance with the foregoing, it appears that the respondent is responsible for the

infringement of the RGPD for the violation of article 32, infringement typified in the

Article 83.4.a) of the same Regulation.

7th

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

certain categories of data controllers or processors", establishes the

Next:

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

are responsible or in charge:

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 State Administration, the Administrations of the autonomous communities

and the entities that make up the Local Administration.

d) Public bodies and public law entities linked to 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 are related

with 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, as well as the political groups of the Local Corporations.

2. When those responsible or in charge listed in section 1 commit any of the

the infractions referred to in articles 72 to 74 of this organic law, the authority of

protection of data that is competent will issue a resolution sanctioning them with

warning. The resolution will also establish the measures to be adopted so that

stop the behavior or correct 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 of which

depends hierarchically, where appropriate, and those affected who had the status of

interested, if any.

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

It will also propose the initiation of disciplinary actions when there are indications

enough for it. In this case, the procedure and the sanctions to be applied will be the

established in the legislation on the disciplinary or sanctioning regime resulting from

app.

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

existence of technical reports or recommendations for treatment that had not been

duly attended to, the resolution in which the sanction is imposed will include a

reprimand with the name of the responsible position and the publication will be ordered in the

Official Gazette of the corresponding State or Autonomous Community.

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

in relation to the measures and actions referred to in the preceding sections.

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

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

this article.

6. When the competent authority is the Spanish Agency for Data Protection, 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 person in charge or

in charge of the treatment that had committed the infraction.

When the competence corresponds to a regional data protection authority,

It will be, in terms of the publicity of these resolutions, to what its regulations have

specific".

It should be noted that the LOPDGDD contemplates in its article 77 the possibility of

warn the person responsible for the infraction and require him to adapt the treatments

of personal data that do not meet your expectations, when those responsible or

data processors listed in section 1 committed any of the

infractions referred to in articles 72 to 74 of this Organic Law.

For this reason, a resolution proposal was prepared so that it is agreed to require the

responsible entity the adoption of the necessary measures to carry out that

adaptation to the personal data protection regulations, preventing the

administrative actions that you carry out can be accessed by people who do not

intervene directly in its formalization. Specifically, when it comes to

administrative notifications, it was warned that such notifications are delivered

directly to the interested party, without the intermediation of other units unrelated to those

have entrusted the action in question; or, if you try that

notification with the collaboration of some other unit, always avoiding that it

can access the content of the act that is notified.

Known this response by the respondent, on the occasion of the hearing process

granted provided a copy of a "Circular" issued by the DPD, regarding the sending of

documentation through electronic communications. Analyzed this Circular

note some improvements in their forecasts, such as the encryption of folders to which

It will be accessed using the password provided to the interested party. However, there are

other instructions that do not meet the requirements mentioned above, such as

are the delivery of documentation through the "direct control" of the interested party or the

sending “open” documents to be signed by the interested party and

returned to the sending unit. The same Circular warns about "practices

inappropriate such as printing or keeping a copy” of the submitted documentation, which

is equivalent to recognizing that the possibility that a third party may access the

documentation is maintained.

Therefore, it is deemed appropriate to require the respondent so that the notifications

that must practice guarantee the confidentiality of the personal data that

they contain.

In this regard, it is noted that not meeting the requirements of this body

can be considered as a serious administrative infraction by “not cooperating with

the Control Authority” before the requirements made, being able to be valued such

conduct at the time of opening an administrative sanctioning procedure.

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: ADDRESS A WARNING to the entity GENERAL DIRECTORATE OF

LA GUARDIA CIVIL, with NIF S2816003D, for an infraction of articles 5.1.f) and

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

SECOND: REQUEST the entity DIRECTORATE GENERAL OF THE CIVIL GUARD,

so that, within a period of one month, counted from the notification of this

resolution, adapt to the personal data protection regulations the operations

processing of personal data that it carries out, with the scope expressed in the

Foundation of Law VII. Within the indicated period, the GENERAL DIRECTORATE OF THE

GUARDIA CIVIL must justify before this Spanish Data Protection Agency

attention to this request.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

THIRD: NOTIFY this resolution to the GENERAL DIRECTORATE OF THE

CIVIL GUARD.

FOURTH

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.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es