 File No.: PS/00465/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the complaining party) dated June 17, 2021

filed a claim with the Spanish Data Protection Agency.

The claim is directed against CITY COUNCIL OF OURENSE with NIF P3205500F

(hereinafter, the claimed party).

The reason on which the claim is based is that the claimant, a union representative by

the SPPME union claims against Local Administration claimed because it does not adopt

the proper security measures in the data management of Police workers

Municipal.

He justifies his statements by stating that the aforementioned council:

publishes data of municipal police officers on the bulletin boards in

the Local Police Headquarters, exposing them to all workers.

the delivery of personal documentation is made in which data of

other colleagues, through unsealed envelopes; Y

has installed a video surveillance system in the garage inside the building, without

having informed the workers about their placement, and despite the fact that there

poster, it does not indicate who is responsible for the treatment or where

You must go to exercise your rights.

As evidence of the reported facts, the following is provided:

-

copy of the Notice Board, where agent data appears, in relation to
to communication of vacation periods; as well as a resolution
denial of vacation request in which a list of
refusals, and it is not a particular communication.

-

an email sent to the DPD of the City Council exposing said situation.

It does not provide images of the location of the cameras.

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 to the claimed party, on 28
of June 2021, and it is reiterated on August 12, 2021, to proceed with its
analysis and report to this Agency within a month, of the actions carried out
carried out to adapt to the requirements set forth in the data protection regulations.

No response has been received to this request.

THIRD: On September 21, 2021, the Director of the Spanish Agency
of Data Protection agreed to admit for processing the claim presented by the
claimant.

FOURTH: On November 10, 2021, the Director of the Spanish Agency
of Data Protection agreed to initiate a sanctioning procedure against the claimed party,

for the alleged infringement of article 5.1.f) of the RGPD, article 32 of the RGPD and article

13 of the RGPD, typified in article 83.5 of the RGPD.

FIFTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written

pleadings stating the following:

In relation to the video surveillance system, it is indicated that the person in charge is the

City Council object of this claim, there are different posters in the building

police with the legend "video surveillance area", both at the entrance of the same, by the

main door as in the entrance to the garage.

The management of the video surveillance system is carried out by personnel from the center itself (a

police), without maintenance being contracted with any company for

part of the Town Hall.

In the garage area of the police offices there are a total of

of 4 cameras not fictitious, but in operation, the conservation period is 1

month.

The activity log sheet can be consulted at the following link: ***URL.1

The images from the cameras can only be viewed "in situ", that is, in the

where the recorder is located, which is a locked room.

The cameras are located in a common area (garage), they have not been installed

nor is there a camera in areas that are not allowed, such as locker rooms,

rest or restrooms.

In relation to the publication on the bulletin board, the city council claimed

wants to state that the notice board is located at the headquarters of the

Headquarters of the Local Police, being the entrance of the same subject to the surveillance of

external personnel and with the appropriate access controls.

These boards exist in the rest of the State Security Bodies and

Autonomous communities.

Its purpose is to announce, facilitate and transfer information of interest to users.
police workers related to the police service forever, such as:
service lists of the days in which the police officers work (with their name, codes
professionals, assigned sections, if they are on statutory rest,
vacations, personal affairs, etc.). Likewise, announcements and
various notices of internal regime, Service Orders, concession lists or
denial of permits with the name of the police (own affairs, festivities,
shift changes and exchanges between police officers, etc.)
In the Security Corps, work is carried out in shifts, both in the morning,
such as afternoon and night and 365 days a year, so it is one of the instruments
that make it possible to provide the information that workers need within a
police organization, as not all of them were on duty neither on the same shifts nor
at the same times.
In the attached photograph, of one of the writings posted on said board and
referring to the holiday period, they appear as in many other advertisements
(previously indicated), the names of the police officials, not data
sensitive or specially protected or others such as telephones, ID,
addresses, emails, etc., in order, in this specific case, to inform the
policemen the situation that, at that time, affected the enjoyment of his period
holiday and this for the purpose of having, sufficiently in advance, the
scheduling of work in the summer season in relation to work-life balance measures

family and work life.

SIXTH: On December 9, 2021, the instructor of the procedure agreed to the

opening of a period of practice tests, considering incorporated the

previous investigation actions, as well as the documents provided by the

reclaimed.

SEVENTH: On January 7, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

IMPOSE the CITY COUNCIL OF OURENSE, with NIF P3205500F, for a

infringement of article 5.1.f) of the RGPD, article 13 of the RGPD and article 32 of the RGPD,

typified in article 83.5, the first two and in article 83.4 of the RGPD the last

of them, a sanction of warning.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: The denounced council makes public personal data of its

workers through the Notice Board of the Local Police Headquarters, indicating

Data relating to communication of denied vacation periods.

Secondly, it is also denounced that the poster for the video-monitored area of the

denounced city hall, does not indicate who is responsible for the treatment and where

address for the exercise of rights.

Thirdly, it is stated that the denounced city council provides information

staff in open envelopes.

SECOND: The city council states in relation to the publication on the Board of

Announcements the respondent wants to state that the bulletin board is one of the

instruments that allow providing the information that workers need within

of a police organization, since not all of them are on duty or in the same

days or at the same times, and which is located at the headquarters of the

Headquarters of the Local Police, being the entrance of the same subject to the surveillance of

external personnel and with the appropriate access controls.

In relation to its video surveillance system, it states that there are different posters

in the police building with the legend "video surveillance area", both at the entrance of the

same, through the front door as in the entrance to the garage and that the cameras are

are located in a common area (garage), and that have not been installed or exist

any camera in areas not allowed such as locker rooms,

rest, or toilets.

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

II

Article 6.1 of the RGPD establishes the assumptions that allow the legalization of the

treatment of personal data.

For its part, article 5 of the RGPD establishes that “personal data will be:

“a) processed in a lawful, loyal and transparent manner in relation to the interested party (“lawfulness,

loyalty and transparency»);

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with those purposes; according to article 89,

paragraph 1, the further processing of personal data for archiving purposes in

public interest, scientific and historical research purposes or statistical purposes are not

deemed incompatible with the original purposes ("purpose limitation");

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which

that are processed ("data minimization");

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

reasonable to eliminate or rectify without delay the personal data that

are inaccurate with respect to the purposes for which they are processed (“accuracy”);

e) kept in a way that allows the identification of the interested parties during

longer than necessary for the purposes of the processing of personal data; the

Personal data may be kept for longer periods provided that it is

processed exclusively for archival purposes in the public interest, research purposes

scientific or historical or statistical purposes, in accordance with Article 89, paragraph 1,

without prejudice to the application of the appropriate technical and organizational measures that

This Regulation is imposed in order to protect the rights and freedoms of the

interested party (“limitation of the retention period”);

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 ("integrity and confidentiality").

The data controller will be responsible for compliance with the provisions of

section 1 and able to demonstrate it (“proactive responsibility”).”

Secondly, it should be noted that the security of personal data comes

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

Article 32 of the RGPD "Security of treatment", establishes that:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

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 confidentiality, integrity, availability and resilience

permanent treatment systems and services;

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

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment 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 account shall be taken of

takes 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 person in charge or the person in charge and

has access to personal data can only process said data following

instructions of the person in charge, unless it is obliged to do so by virtue of the Right of

the Union or 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

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.

(…)"

Thirdly, in relation to the information to be provided when the data

data are obtained from the interested party, article 13 of the RGPD establishes the following:

"1. When personal data relating to him is obtained from an interested party, the

responsible for the treatment, at the time these are obtained, will provide

all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their

representative;

b) the contact details of the data protection delegate, if any;

c) the purposes of the treatment to which the personal data is destined and the legal basis

of the treatment;

d) when the treatment is based on article 6, paragraph 1, letter f), the interests

legitimate of the person in charge or of a third party;

e) the recipients or the categories of recipients of the personal data, in their

case;

f) where appropriate, the intention of the controller to transfer personal data to a third party

country or international organization and the existence or absence of a decision to

adequacy of the Commission, or, in the case of transfers indicated in the

Articles 46 or 47 or Article 49, paragraph 1, second paragraph, reference to the

adequate or appropriate warranties and the means to obtain a copy of these or

to the fact that they have been borrowed.

2. In addition to the information mentioned in section 1, the person responsible for the

treatment will facilitate the interested party, at the moment in which the data is obtained

personal, the following information necessary to guarantee data processing

fair and transparent

a) the period during which the personal data will be kept or, when it is not

possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access to the

personal data relating to the interested party, and its rectification or deletion, or the limitation

of its treatment, or to oppose the treatment, as well as the right to portability

of the data;

c) when the treatment is based on article 6, paragraph 1, letter a), or article

9, paragraph 2, letter a), the existence of the right to withdraw consent in

any time, without affecting the legality of the treatment based on the

consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or a

necessary requirement to sign a contract, and if the interested party is obliged to provide

personal data and is informed of the possible consequences of not

provide such data;

f) the existence of automated decisions, including profiling, to which

referred to in article 22, sections 1 and 4, and, at least in such cases, information

about applied logic, as well as the importance and consequences

provisions of said treatment for the interested party.

3. When the data controller plans further data processing

personal data for a purpose other than that for which they were collected, you will provide the

interested party, prior to such further processing, information on that other purpose

and any additional information relevant under paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in the

to the extent that the interested party already has the information."

In this sense, reporting on video surveillance according to the RGPD is an obligation.

included in this legislative framework.

An informative device must be available in a visible area (eg access door)

indicating that it is a video-monitored area, it must indicate the

existence of the treatment, the identity of the person in charge, as well as the possibility of

exercise the rights provided for in articles 15 to 22 of the Regulation (EU)

2016/679.

The image of a person to the extent that it identifies or can identify the person

constitutes personal data, which may be processed to di-

various purposes.

Article 22 of Organic Law 3/2018 (December 5)-LOPDGDD- provides:

"1. Natural or legal persons, public or private, may carry out the

processing of images through camera systems or video cameras with the purpose of

to preserve the safety of people and property, as well as its installations.

nes.

The AEPD, in a related report, stipulates that it is not necessary for cartels to be

stand right below the cameras. It is enough to do it in a visible place and that it includes

open and closed spaces where the video camera circuit is operational.

This badge will be displayed in a visible place, and at least, at the entrances to the areas

guarded whether indoors or outdoors. In the event that the video-monitored space has

has several accesses, said video-surveillance area badge must be available

in each one of them.

III

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

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

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

who are responsible or in charge:

a) The constitutional bodies or those with constitutional relevance and the institutions of

autonomous communities analogous to them.

b) The jurisdictional bodies.

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

autonomous 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 are

related to the exercise of powers of public law.

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Legislative Assemblies

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

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 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 of the

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

interested party, if any.

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

data will also propose the initiation of disciplinary actions when there are

sufficient evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on disciplinary or sanctioning regime that

result of application.

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

proves the existence of technical reports or recommendations for the treatment 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 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 person in charge or in charge of the treatment that had committed the infraction.

When the competence corresponds to a regional authority for the protection of

data will be, in terms of the publicity of these resolutions, to what your

specific regulations".

IV

In the present case, it has been verified through the documentation in the

file that the defendant violated article 5 of the RGPD, principles related to the

treatment, in relation to article 5 of the LOPGDD, duty of confidentiality, when

post on the police bulletin board, names and surnames of agents.

In view of what is indicated by the claimed party, in addition to the publication of the lists

with names and surnames, there is information referring to natural persons that should not be

be published as it goes beyond the mere organizational purpose of the work, for

example, the vacations or the own affairs or permissions of each one, are all of them

matters of merely personal interest, and not public.

In addition, all this information, if it continues to be published, will be linked to other data such as the

license plate number or DNI, which unequivocally identifies the agent and can

be well known by their peers in the workplace.

It is considered that the processing of personal data by the complained party has

clearly exceeded the purpose for which they were given, mainly in the field of

of vacations, permits and own affairs.

In this regard, it should therefore be noted that it is not necessary to publish all the data

that appear on the bulletin board to achieve the organizational purpose pursued

by the claimed party, and that is perfectly compatible with fulfilling the duty

of confidentiality.

The duty of confidentiality must be understood as having the purpose of preventing

carry out leaks of personal data without the consent of their owners.

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.

Second, there are clear indications that the respondent has violated the

article 32 of the RGPD, upon delivery of personal documentation containing data

from other colleagues, by means of unsealed envelopes, allowing access to the

themselves with breach of the established measures.

The liability of the claimed party is determined by the security breach

revealed by the claimant, since he is responsible for making decisions

aimed at effectively implementing the technical and organizational measures

appropriate to guarantee a level of security appropriate to the risk to ensure the

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

in the event of a physical or technical incident. However, from the documentation

contributed, it follows that the entity has not only failed to comply with this obligation, but also

In addition, the adoption of measures in this regard is unknown, despite having given

transfer of the claim filed.

Therefore, it is estimated that the defendant would be presumably responsible for the infringement

of the RGPD: the violation of article 32, offense typified in its article 83.4.a).

In relation to the video surveillance system of the defendant, he states that the

camera images can only be viewed "in situ", that is, in the place

where the recorder is located, that it is a locked room and that said

cameras are located in a common area (garage), they have not been installed or

There is no camera in areas that are not allowed, such as locker rooms,

rest or restrooms.

However, it is considered that the respondent party has a system of

video surveillance, whose informative badge presents irregularities by not accrediting

by the data controller despite your request, an address

where to exercise legally regulated rights.

The known facts could constitute an infringement, attributable to the party

claimed for violation of the content of art. 13 GDPR.

v

The violation of article 5 of the RGPD is typified in article 83.5 a) of the

RGPD, considers that the infringement of “the basic principles for the treatment,

including the conditions for consent under 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 a maximum of €20,000,000 or, in the case of

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

global annual total 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 article 5 of Regulation (EU) 2016/679.

(…)"

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

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 71, Violations, states that:

"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 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, 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 technical and organizational measures that have been implemented as required by article 32.1 of Regulation (EU) 2016/679".

The violation of article 13 of the RGPD is typified in article 83.5.b) of the RGPD establishes that:

"The infractions of the following dispositions 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:

b) the rights of the interested parties pursuant to articles 12 to 22;"

In turn, article 74.a) of the LOPDGDD, under the heading "Infringements considered mild has:

"They are considered minor and the remaining infractions of a legal nature will prescribe after a year. merely formal of the articles mentioned in paragraphs 4 and 5 of article 83 of Regulation (EU) 2016/679 and, in particular, the following:

a) Failure to comply with the principle of transparency of information or the right of information of the affected party for not providing all the information required by

Articles 13 and 14 of Regulation (EU) 2016/679."

SAW

Therefore, the facts that are the subject of this claim prove the existence of

infraction by the claimed party by violating the provisions of articles 5.1.f), 32.1 and

13 of the GDPR.

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: THAT the CITY COUNCIL OF OURENSE, with NIF P3205500F, by

infringement of article 5.1.f) of the RGPD, article 13 of the RGPD and article 32 of the RGPD,

typified in article 83.5, the first two, and in article 83.4 of the RGPD the last

of them, a sanction of warning is imposed for each one.

SECOND: REQUEST the CITY COUNCIL OF OURENSE, with NIF P3205500F, to

protection of the provisions of article 58.2 d) of the RGPD, which adopts the measures

necessary to update your "Privacy Policy" to current regulations on

personal data protection, -Regulation (EU) 2016/679 (RGPD)-, adapting

the information offered to the requirements contemplated in article 13 of the RGPD,

must provide users, prior to the collection of data

of the same, all the information required in the aforementioned precept, for which

that the claimed party must take into account the provisions of article 6 of the RGPD

in relation to the legality of the treatment, as well as what is indicated in article 5 of the

RGPD in relation to the purpose of the treatment and term of conservation of the data.

The text of the resolution establishes the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of

data, from which it is clearly inferred what measures to adopt, without prejudice

that the type of specific procedures, mechanisms or instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

treatment who fully knows your organization and has to decide, based on the

proactive responsibility and risk approach, how to comply with the RGPD and the

LOPDGDD.

Said measures must be adopted within a period of one month computed from the date

in which this sanctioning resolution is notified, and the means must be provided

proof of compliance.

THIRD: COMMUNICATE this resolution to the Ombudsman,

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

FOURTH: NOTIFY this resolution to the CITY COUNCIL OF OURENSE.

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es