 Procedure No.: PS/00128/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: The claim filed by D. A.A.A. (hereinafter, the claimant)

has entry dated 05/07/2019 in the Spanish Agency for Data Protection.

The claim is directed against CITY COUNCIL OF ***LOCALITY.1, with NIF

P3002000B (hereinafter the claimed one). The grounds on which the claim is based are

In summary: that on 03/20/2019 he sent a letter to the respondent requesting information

on certain questions related to the control of signing by fingerprint

fingerprint, without having received a response to the request made to date.

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

Data Inspection proceeded to carry out the following actions:

On 07/01/2019, the claim submitted was transferred to the defendant for analysis

and communication to the complainant of the decision adopted in this regard. Likewise, it

required him to send to the determined Agency within a period of one month

information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

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

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant.

On 08/08/2019, in response to the request for information, Document was

Security where it is reported in accordance with the provisions of the RGPD and indicates,

among others, that the agency used to control presence and access to its

installations a fingerprint detection system that does not perform in any

moment a biometric analysis, but it elaborates an identification algorithm as a result of

a reading of several points of the personal fingerprint and that the data of the algorithm does not

they cannot be decrypted or disassembled by any unauthorized entity.

And in response to a new request for information, in a letter dated 10/21/2019, it provided the

report on impact assessment in the treatment of fingerprint data

to control the presence of employees.

THIRD: On 11/25/2019, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed.

FOURTH: On 09/30/2020, the Director of the Spanish Protection Agency

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

infringement of article 13 of the RGPD, contemplated in article 83.5.b) of the aforementioned

Regulation, considering that the sanction that could correspond would be that of

warning.

FIFTH: Once the initiation agreement has been notified, the one claimed at the time of this

The resolution has not presented a written statement of allegations, for which reason the

indicated in article 64 of Law 39/2015, of October 1, on the Procedure

Common Administrative Law of Public Administrations, which in section f)

establishes that in the event of not making allegations within the period established on the

content of the initiation agreement, it may be considered a proposal for

resolution when it contains a precise statement about the responsibility

imputed, reason why a Resolution is issued.

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

accredited the following:

PROVEN FACTS

FIRST: On 05/07/2019 there is a written entry in the AEPD presented by the

interested party against the defendant stating that on 03/20/2019 he addressed the same

requesting information on the control of signing by fingerprint of

in accordance with the provisions of the data protection regulations of

personal nature, without a response to said date having been obtained to date.

request.

SECOND: It consists provided by the claimant letter addressed to the claimed requesting

the information in accordance with the RGPD.

THIRD: Evidence provided by the respondent in writing dated 10/21/2019 Report

Evaluation of the Impact of the treatment of the data of the fingerprint for control of

presence of employees. Likewise, it provides a security document and a

company Syon, Solutions & Identification, on fingerprints of the

workers.

FOUNDATIONS OF LAW

Yo

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

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

Law 39/2015, of October 1, on the Common Administrative Procedure of

the Public Administrations, in its article 64 "Agreement of initiation in the

procedures of a sanctioning nature", provides:

II

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the rules

regulators of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible

rating and sanctions that may apply, without prejudice to what

result of the instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that

attribute such competence, indicating the possibility that the presumed

responsible can voluntarily acknowledge their responsibility, with the

effects provided for in article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those that

may be adopted during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the

procedure and the deadlines for its exercise, as well as an indication that, in

If you do not make allegations within the stipulated period on the content of the

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the responsibility

imputed.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out in a phase

later by drawing up a List of Charges, which must be notified to

the interested".

In application of the previous precept and taking into account that no

formulated allegations to the initial agreement, it is appropriate to resolve the initiated procedure.

The legitimacy for the treatment of the fingerprint for the control of the

workers by the employer we must look for it in articles 9 and 6 of the RGPD.

III

Article 9 of the RGPD establishes in its sections 1 and 2.b) the following:

"1. The processing of personal data that reveals the origin

racial or ethnic origin, political opinions, religious or philosophical convictions, or

union affiliation, and the processing of genetic data, biometric data aimed at

uniquely identify a natural person, data related to health or data

relating to the sexual life or sexual orientations of a natural person.

2. Section 1 will not apply when one of the

following circumstances:

b) the treatment is necessary for the fulfillment of obligations and the

exercise of specific rights of the person in charge of the treatment or of the interested party in

the field of labor law and social security and protection, to the extent

that is authorized by the Law of the Union of the Member States or a convention

in accordance with the law of the Member States that establishes guarantees

respect for fundamental rights and the interests of the

interested."

Article 6.1.b) of the RGPD indicates:

"1. The treatment will only be lawful if at least one of the following is met

conditions:

b) the treatment is necessary for the execution of a contract in which the

interested party is a party or for the application at the request of the latter of measures

pre-contractual."

The defendant has legitimacy, based on the aforementioned regulations, to

carry out the labor control of its workers, provided that it meets the requirements

indicated in the sixth Legal Basis.

The claimed facts suppose the violation by the City Council of

what is stated in article 13 of the RGPD, by not informing of the treatment provided for in

in relation to the control of signing by fingerprint, in accordance with the

pronouncements established in the aforementioned article.

This article determines the information that must be provided to the interested party

at the time of collecting your data, establishing the following:

Article 13. Information that must be provided when personal data is

obtain from the interested party.

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 basis

legal treatment;

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

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

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

in your case;

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

third country or international organization and the existence or absence of a

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

indicated in articles 46 or 47 or article 49, paragraph 1, second paragraph,

reference to adequate or appropriate safeguards and means of obtaining

a copy of these or the fact that they have been loaned.

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 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 related 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 data portability;

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

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

consent at any time, without affecting the legality of the

treatment based on 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 providing such data;

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

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

significant information about the applied logic, as well as the importance and

anticipated consequences of said treatment for the interested party.

3. When the person in charge of the treatment projects the subsequent treatment of

personal data for a purpose other than that for which it was collected,

will provide the interested party, prior to said further treatment, information

for that other purpose and any additional information relevant to the meaning of paragraph 2.

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

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

In the present case, the claimant addressed the respondent in writing

requesting information on the control of signing by fingerprint,

IV

considering that it could be violating the regulations on the protection of

data without obtaining a response to said request.

The documentation provided to the file does not include the response offered to the

claimant and, as stated in the second antecedent in response to the

information request sent by the AEPD the respondent provides Document is

Security in accordance with the provisions of the RGPD, noting that the body

local used said system of control of presence and access to its facilities that

does not entail at any time a biometric analysis, but rather a

identification algorithm based on a reading of several points of the personal fingerprint and

that the algorithm data cannot be decrypted or disassembled by any

unauthorized entity. Likewise, the report on Impact Assessment was provided.

in the treatment of the data of the fingerprint for the control of the presence of the

employees.

In relation to the issues raised in this case, first of all

It should be noted that the implementation and integration of a time control system

based on the fingerprint by the employer, has to be informed to the

employees in a complete, clear, concise manner and, in addition, the aforementioned information must

be completed with reference to both the legal bases that cover said type

of access control, as well as the basic information referred to in the

article 13 of the RGPD.

In the case examined, it is true that there is no record of the respondent's response to the

document presented by the claimant in which he requested to be informed of the moment in

that the information was provided to the workers of the fingerprint registration system

fingerprint and reiterate such information.

Second, the installation of a control system based on the collection

and treatment of the fingerprint of the employees implies the treatment of their data

personal since personal data is all information about a person

physical identified or identifiable in accordance with article 4.1 of the RGPD.

As for the fingerprint, it is also about data that must be qualified.

two as biometric data and in accordance with article 4.14 of the RGPD have this

consideration when they have been “obtained from a technical treatment

specific, relating to the physical, physiological or behavioral characteristics of a

natural person that allow or confirm the unique identification of said person,

such as facial images or fingerprint data.

This means that, in accordance with article 9.1 of the RGPD, in the case

present, the specific regime provided for special categories is applied to them

of data provided for in article 9 of the RGPD.

In this sense, recital 51 of the RGPD highlights the nature

restrictive with which the treatment of this data can be admitted:

“(51) ... Such personal data should not be processed, unless it is allowed

their treatment in specific situations contemplated in this Regulation,

given that Member States may lay down provisions

specific on data protection in order to adapt the application of the

rules of this Regulation to the fulfillment of a legal obligation or to the

fulfillment of a mission carried out in the public interest or in the exercise of powers

data conferred on the data controller. In addition to the requirements

specific to that treatment, the general principles and other

rules of this Regulation, in particular as regards the conditions of

legality of the treatment. Exceptions to the

general prohibition of treatment of those special categories of personal data,

among other things when the interested party gives his explicit consent or in the case of

specific needs, in particular when the treatment is carried out in the

framework of legitimate activities by certain associations or foundations whose

objective is to allow the exercise of fundamental freedoms.

And recital 52 states that

“(52) Likewise, exceptions to the prohibition of treating

special categories of personal data when established by the Law of the

Union or of the Member States and provided that the appropriate guarantees are given, in order to

to protect personal data and other fundamental rights, when it is in the interest

public, in particular the processing of personal data in the field of legislation

employment, legislation on social protection, including pensions and for purposes of

security, supervision and health alert, prevention or control of diseases

communicable diseases and other serious threats to health…”

In accordance with these considerations, the treatment of biometric data of

special categories will require, in addition to the concurrence of one of the bases

legal provisions established in article 6 of the RGPD, any of the exceptions provided

in article 9.2 of the RGPD.

The analysis of the legal basis of legitimacy to carry out this treatment comes

of article 6 of the RGPD, regarding the legality of the treatment, which in its section 1, letter

b) states: "The treatment will be lawful if at least one of the following is met:

conditions: (...) b) the treatment is necessary for the execution of a contract in the

that the interested party is a party or for the application at the request of the latter of measures

pre-contractual (…)”.

By virtue of this precept, the treatment would be lawful and would not require the

consent, when the data processing is carried out for the fulfillment of

labor contractual relationships.

This precept would also cover the data processing of

public employees, even if their relationship is not contractual in the strict sense. There are

It should be noted that sometimes, in order to fulfill its obligations in relation to

with public employees, the Administration must carry out treatment of

certain data referred to in the RGPD, in its article 9, as "categories

special data”.

On the other hand, and as highlighted in recital 51 of the same RGPD,

to the extent that the biometric data are of a special category in the cases

of biometric identification (art. 9.1 RGPD), it will be necessary that one of the

the exceptions provided for in article 9.2 of the RGPD that would allow lifting the general prohibition of the treatment of these types of data established in the article 9.1.

At this point, special mention must be made of letter b) of article 9.2 of the RGPD, according to which the general prohibition of biometric data processing does not It will apply when "the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the data controller or of the interested party in the field of labor law and social security and protection, to the extent authorized by the Law of the Union of the Member States or a collective agreement in accordance with the law of the Member States establishing adequate guarantees of respect for fundamental rights and the interests of the interested".

In the Spanish legal system, article 20 of the Consolidated Text of the Statute of workers (TE), approved by Royal Legislative Decree 2/2015, of 23 October, provides for the possibility for the employer to adopt surveillance measures and control to verify compliance with the labor obligations of their workers:

"3. The employer may adopt the measures it deems most appropriate monitoring and control to verify compliance by the worker with their obligations and labor duties, keeping in its adoption and application the consideration due to their dignity and taking into account, where appropriate, the real capacity of the workers with disabilities".

And in the Basic Statute of the Public Employee, approved by Royal Decree

Legislative 5/2015, of October 30, in its article 54 in relation to the principles of

"The unemployment of tasks

conduct of public employees states:

corresponding to his job will be highlighted diligently and in compliance with the

established day and time

It should also be noted that the basic legislation of the local regime attributes to the

Mayor President of the Corporation the direction of the government and administration

municipal as well as exercise the superior direction of the personnel at the service of the

Municipal administration.

The possibility of using data-based systems is undeniable

biometrics to carry out access and time control, although it does not seem

that it is or should be the only system that can be used: thus the use of cards

personal codes, the use of personal codes, the direct visualization of the point of

marking, etc., which may constitute, by themselves or in combination with any of the

the other available systems, equally effective measures to carry out the

control.

In any case, prior to the decision on the start-up

of such a control system and taking into account its implications,

processing of biometric data aimed at uniquely identifying a

natural person, it would be mandatory to carry out an impact assessment regarding the

protection of personal data to assess both the legitimacy of the

treatment and its proportionality such as the determination of existing risks and

the measures to mitigate them in accordance with the provisions of article 35 RGPD.

In the present case, it must be stated that the entity has accredited the

mandatory impact assessment related to data protection regulated in the

article 35 of the RGPD providing the corresponding document.

Biometric data is closely linked to a person, given

that they can use a certain unique property of an individual for their

identification or authentication.

SAW

According to Opinion 3/2012 on the evolution of biometric technologies,

“Biometric data irrevocably changes the relationship between the body and

identity, as they make the features of the human body legible

by machines and are subject to further use.”

In relation to them, the Opinion specifies that different types of

treatments by pointing out that "Biometric data can be processed and stored in

different ways. Sometimes the biometric information captured from a person is

stored and treated raw, which allows the source from which it comes to be recognized without

special knowledge; for example, a photograph of a face, a photograph of a

fingerprint or voice recording. Other times, raw biometric information

captured is treated in such a way that only certain characteristics or traits are extracted and

they are saved as a biometric template.”

The processing of this data is expressly permitted by the RGPD

when the employer has a legal basis, which is usually the

Work contract. In this regard, the STS of July 2, 2007 (Rec. 5017/2003), has

legitimate understanding of the treatment of biometric data carried out by the Administration

for the time control of its public employees, without the need for

prior consent of the workers.

However, the following should be noted:

O The worker must be informed about these treatments.

O The principles of purpose limitation, necessity,

proportionality and minimization of data.

In any case, the treatment must also be adequate, pertinent and not

excessive for that purpose. Therefore, biometric data that is not

necessary for that purpose should be abolished and the creation will not always be justified.

of a biometric database (Opinion 3/2012 of the Art. 29 Working Group).

O Use of biometric templates: Biometric data should be stored

as biometric templates whenever possible. The template must be extracted from

a way that is specific to the biometric system in question and not used

by other controllers of similar systems in order to ensure that

a person can only be identified in biometric systems that have

a legal basis for this operation.

O The biometric system used and the security measures chosen must

ensure that reuse of the biometric data in question is not possible

for another purpose.

O Mechanisms based on encryption technologies should be used in order to

prevent unauthorized reading, copying, modification or deletion of biometric data.

O Biometric systems should be designed in such a way that they can be revoked

the identity bond.

O You should choose to use specific data formats or technologies that

prevent the interconnection of biometric databases and the disclosure of data

not checked.

O Biometric data must be deleted when they are not linked to the

purpose that motivated its treatment and, if possible, should be implemented

automated data deletion mechanisms.

SAW

Article 83.5. b) of the RGPD, considers that the infringement of “the rights of

those interested in accordance with articles 12 to 22”, is punishable, in accordance with the

section 5 of the aforementioned article 83 of the aforementioned Regulation, "with fines

administrative fees of €20,000,000 maximum or, in the case of a company, a

amount equivalent to a maximum of 4% of the total global annual turnover of the

previous financial year, opting for the highest amount.

The LOPDGDD in its article 71, Violations, states that:

“The acts and behaviors referred to in the regulations constitute infractions.

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

The LOPDGDD in its article 72 indicates for prescription purposes: "Infringements

considered very serious:

"1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

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

particularly the following:

(…)

h) The omission of the duty to inform the affected party about the treatment of their

personal data in accordance with the provisions of articles 13 and 14 of the

Regulation (EU) 2016/679 and 12 of this organic law.

(…)"

7th

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/13

However, the LOPDGDD in its article 77,

Regime applicable to

certain categories of controllers or processors, establishes the

Next:

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

of which they are responsible or entrusted:

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

institutions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

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

autonomous communities and the entities that make up the Local Administration.

d) Public bodies and public law entities linked or

dependent on the Public Administrations.

e) The independent administrative authorities.

f) The Bank of Spain.

g) Public law corporations when the purposes of the treatment

related to the exercise of powers of public law.

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

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

Autonomous Legislative, as well as the political groups of the Corporations

Local.

2. When the managers or managers listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

also the measures that should be adopted to stop the behavior or correct it.

the effects of the infraction that had been committed.

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

body on which it reports hierarchically, where appropriate, and those affected who have

the condition of interested party, if any.

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

data protection will also propose the initiation of disciplinary actions

when there is sufficient evidence to do so. In this case, the procedure and

sanctions to apply will be those established in the legislation on disciplinary regime

or sanction that results from application.

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

and the existence of technical reports or recommendations for treatment is proven

that had not been duly attended to, in the resolution imposing the

The sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or Autonomous Gazette that

correspond.

4. The data protection authority must be informed of the

resolutions that fall in relation to the measures and actions referred to

the previous sections.

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

analogous of the autonomous communities the actions carried out and the

resolutions issued under this article.

6. When the competent authority is the Spanish Agency for the Protection of

Data, it will publish on its website with due separation the resolutions

referred to the entities of section 1 of this article, with express indication of the

identity of the person in charge or in charge of the treatment that would have committed the

infringement.

When the competence corresponds to a regional protection authority

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

its specific regulations.

In the case that concerns us and as indicated previously, the

This sanctioning procedure shows that the defendant has not informed

adequately in relation to the control of presence and access to its facilities

municipal authorities through a fingerprint system, an arbitrated procedure where the

affected develops its activity.

In accordance with the evidence available to said conduct

constitutes an infringement of the provisions of article 13 of the RGPD.

However, the RGPD, without prejudice to the provisions of article 83,

contemplates in its article 77 the possibility of resorting to the sanction of warning

to correct the processing of personal data that is not in accordance with your

forecasts, when those responsible or in charge listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law.

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:

***LOCATION.1, with NIF

FIRST: IMPOSE the CITY COUNCIL OF

P3002000B, for an infringement of article 13 of the RGPD, typified in article

83.5.b) of the RGPD, a penalty of warning in accordance with article 77.2

of the LOPDGDD.

SECOND: NOTIFY this resolution to the CITY COUNCIL OF

***LOCATION.1, with NIF P3002000B.

: REQUEST the CITY COUNCIL OF ***LOCALITY.1, with NIF

THIRD

P3002000B, so that within a month from the notification of this resolution,

accredits before the AEPD the adoption of the necessary and pertinent measures to

correct the processing of personal data that is not in accordance with the regulations in

matter of protection of personal data and prevent their recurrence

violations such as those that have given rise to the claim correcting the effects of

infringement, establishing the necessary measures to adapt to the requirements

contemplated in article 13 of the RGPD.

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, the

This Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art.

48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the

LPACAP, the interested parties may optionally file an appeal for reconsideration

before the Director of the Spanish Agency for Data Protection within a period of

month from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the agency

[https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es