-File No.: EXP202100354

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the complaining party) dated 06/14/2021

filed a claim with the Spanish Data Protection Agency. The

The claim is directed against the CITY COUNCIL OF SALINAS DE PISUERGA with NIF

P3415800F (hereinafter claimed). The grounds on which the claim is based are

the following: the claimant states that the respondent has given a third party access

to the administrative file in which a construction work promoted

by the claimant; said person, member of the Citizen Council of the municipality,

stated at a meeting of the same that the claimant should adhere to the execution of his

project according to the provisions of the report submitted and approved; the claimant indicates

How can that person know the details of the file, stating that

There is no formal request for access to it in the Registry, so

you understand that you have accessed the information irregularly; also points out that

has published the minutes of the meeting of the Citizen Council on the facebook page and

it contains your first and last name without your consent.

And it provides:

- Minutes of the Citizen Council meeting held on ***DATE.1.

- Photograph of the Facebook page in which the publication of the

mentioned minutes of the meeting of the Citizen Council.

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, to

to proceed with its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

The complainant in writing sent to this Agency dated 07/22/2021 has indicated the

Next:

"In relation to "the report presented and approved" it should be reported that the person,

member of the Citizen Council who made that observation, has never had access to

that file from this town hall.

We do not know how he knows it, but it is easy to imagine that in the case of a town and a

a work of such little entity and importance and being the neighbor of the

claimant, at any time or place has been able to hear it.

In relation to the minutes of the Citizen Council, in which the name of the

claimant, it should be noted that the publication of the minutes is an exercise in transparency

of the public and that in no case can it be understood that there is an affectation to the honor or

the moral integration of the claimant and much less an attack on his dignity, nor

impairment of fundamental rights.

In the future, this council, which will continue in its exercise of transparency, will omit

any name that can offend sensitivities."

THIRD: On 07/23/2021, in accordance with article 65 of the LOPDGDD,

the claim filed by the claimant was admitted for processing.

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 57.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the

following ends:

With dates 08/30, 31/2021 and 09/30/2021, the respondent has provided the following

information:

Regarding the procedure for registration and consultation of information and documentation

that works in the administrative files of requests for work presented by the

citizens, there are two procedures, one external and one internal.

At an external level to the town hall, to be able to consult a file

administrative, the interested party must previously make a request through

from the face-to-face registry office or through the registry office at the headquarters

City Hall electronics. Once the consultation request has been authorized, you will be

facilitates in the municipal dependencies in person the consultation to the

proceedings. At no time is a copy of the file provided.

Internally, the query is made through the management tool of

Manage files, the users registered to carry out the query are

the city council secretary, administrative assistant and the mayor. In addition, the

Files are also filed in folders which can be

consulted in person by the members of the corporation and

city hall staff. Both staff and the corporation have signed

the commitment of confidentiality.

Access to the tool is done through an electronic certificate or

name and password and has an access log.

There are no records of access to paper files by

the corporation or public employees

- A copy of the records of accesses made to the file is provided

automated corresponding to the dates from 02/06/1019 to

08/25/2021, from which it follows that all accesses to the file have

been carried out by two users who, according to statements by the representative

of the City Council are personnel with authorized access and access is part

of their duties in the performance of their job.

- Provide a copy of the record of treatment activity called "REGISTRATION

OF ENTRY AND OUTPUT OF DOCUMENTATION".

- Regarding the security measures, they state that the file manager

used is the managed electronic administration tool, certified

in accordance with the National Security Scheme with HIGH category,

with the AENOR certificate of qualified trust service provider,

ISO 27001 Information Security certification and compliance

of the GDPR.

Likewise, it states that all workers have signed a commitment

of confidentiality.

- Provides a copy of the risk analysis that contemplates the treatment "Management

administration of urban discipline records".

The risk analysis report includes the identified threats to which

personal data is exposed, as well as the vulnerabilities that

they can take advantage of such threats to succeed. It has also been estimated

the damage that could be caused by the different threats in the event that

materialize, as well as the probability of its occurrence. With these data,

an estimate of the level of risk has been made and decisions have been made

to manage these risks by implementing security measures

that eliminate or reduce those risks that it has been decided to manage.

Regarding the security measures included in the risk analysis

relating to supports and documents establishes that:

o The storage devices of the supports and documents that

contain personal data must have

mechanisms that hinder its opening, by means of keys or other

means that perform the same function.

o Only authorized users should have the keys and means

that facilitate the opening of said devices.

o When the physical characteristics do not allow this measure to be adopted,

shall take the necessary measures to prevent the access of

unauthorized persons.

o As long as the documents with personal data are not

archived in the indicated storage devices

previously, because it is in the process of being processed, the people who

are in their charge must guard them and prevent access by

unauthorized persons.

Regarding the security measures included in the risk analysis

related to access control establishes, among others, that:

o The staff will only access those data and resources that they need to

the development of its functions.

o Mechanisms must be established to prevent a user from

access resources with rights other than those authorized. sayings

mechanisms, in the case of computer media, may consist of the

assignment of passwords for access to them, or other

more sophisticated devices: biometrics, USB keys, etc.; and in the case

of paper documents, in the delivery of keys that facilitate the

opening of the storage devices where the data is collected

information.

FIFTH: On 02/18/2022, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the one claimed by the alleged

Infractions of articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a)

and 83.4.a) of the aforementioned RGPD.

SIXTH: Notified of the initiation agreement on 03/09/2022, the respondent submitted a written

of allegations stating that as he already indicated in his day, no one was ever given

access to any file that had not been requested through the channel

regulatory; that the citizen council member cited had never applied for the

mentioned file and had never had access to it; which was published in

Facebook an act of the citizen council for the sake of transparency of the

public performances and it contains information with names and surnames that, in

no case affects dignity or reveals any secret, because what is published is public

and notorious, nor can it be considered harmful to the interests or honor of anyone; when

the person in charge of the Diputación de Palencia for data protection requested that

removed the data to which we refer and it was removed immediately; who understands

that it is not possible to initiate a sanctioning process.

SEVENTH: On 03/16/2022, it was agreed to open a practice period for

tests, 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 the file.

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

home submitted by the claimed party and the accompanying documentation.

EIGHTH: On 07/12/2022, a Resolution Proposal was issued in the sense that by

the Director of the AEPD will sanction the person claimed for infraction for infraction of the

articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the

RGPD, with a sanction of warning.

After the period established for presenting allegations by the defendant, there was no

submitted any writing.

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

accredited the following.

PROVEN FACTS

FIRST. On 06/14/2021 it has entry in the Spanish Agency for the Protection of

Written data of the claimant stating that the claimed party has given to a third party

access to the administrative file in which a construction work is regulated

driven by the claimant; said person, a member of the Citizen Council of the

municipality, stated at a meeting of the same that the claimant should adhere to the

execution of your project according to the provisions of the report presented and approved; the

claimant wonders how such a person could know the details of the

file, if the Registry does not contain any formal request for access to it,

so you understand that you have accessed the information irregularly; likewise,

declares that the minutes of the meeting of the Citizen Council have been published in the

facebook page and it contains your name and surname without your consent.

SECOND. The Minutes of the meeting of the Citizen Council held on

***DATE.1 in whose section, Requests and Questions, what is indicated by the

claimant in his brief.

THIRD. The respondent in writing dated 06/21/2021 has stated that “the person,

member of the Citizen Council who made that observation, has never had access to

that file from this town hall.

We do not know how he knows it, but it is easy to imagine that in the case of a town and a

a work of such little entity and importance and being the neighbor of the

claimant, at any time or place has been able to hear it.

In relation to the minutes of the Citizen Council, in which the name of the

claimant, it should be noted that the publication of the minutes is an exercise in transparency

of the public and that in no case can it be understood that there is an affectation to the honor or

the moral integration of the claimant and much less an attack on his dignity, nor

impairment of fundamental rights.

In the future, this council, which will continue in its exercise of transparency, will omit

any

sensitivities".

Name

can

hurt

that

FOURTH. There is a screenshot provided of the Facebook page in which

The publication of the minutes of the Citizen Council meeting is included.

FIFTH. The respondent in writing dated 03/08/2022 has stated that "Certainly

published on Facebook an act of the citizen council for the sake of transparency of the

public performances. In said record, information appeared with names and surnames

that, in no case affects dignity or reveals any secret, since what is published is

public and notorious, nor can it be considered harmful to the interests or honor of anyone.

Furthermore, when the person in charge of the Diputación de Palencia for the

data protection requested this town hall to withdraw the data to which we

we refer, it was withdrawn immediately.

SIXTH. A copy of the Risk Analysis has been provided; the treatment "Management

administration of urban discipline records".

FOUNDATIONS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter RGPD), grants each autho-

authority of control and according to what is established in articles 47, 48.1, 64.2 and 68.1 of the Law

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

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures

Data processed by the Spanish Agency for Data Protection will be governed by the provisions

established in Regulation (EU) 2016/679, in this organic law, by the provisions

regulatory provisions issued in its development and, as long as they do not contradict them, with

subsidiary character, by the general rules on administrative procedures

you."

II

In the present case, the facts revealed by the claimant are

materialize in that the defendant would have enabled a third party to access the experience

administrative tooth in which a work promoted by the claimant is regulated, as well

such as the dissemination of your personal data on the Facebook page of the claimed party.

Article 58 of the RGPD, Powers, states:

"two. Each control authority will have all the following powers:

rectives listed below:

(…)

b) sanction any person responsible or in charge of the treatment with a warning

when the treatment operations have violated the provisions of the

this Regulation;

(...).”

The RGPD establishes in article 5 the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

The article notes that:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing

to and against accidental loss, destruction or damage, through the application of

appropriate technical or organizational measures (“integrity and confidentiality”)”.

(…)

III

The documentation in the file offers indications that the claimant

do, violated article 5 of the RGPD, principles related to treatment, in relation to

Article 5 of the LOPGDD, duty of confidentiality, when proceeding to the publication of

your data on the Facebook page of the claimed party.

As it appears in the proven facts, a screen print is provided

of the Facebook page where the minutes of the meeting of the

Citizen Council, where the personal data of the claimant is contained.

tea.

The duty of confidentiality, previously the duty of secrecy, must understand-

It is known that its purpose is to avoid leaks of data without consent.

given by the holders of the same, as well as to avoid leaks of the

data or transfers of the same to third parties without the existence of a legal basis that

legitimate.

However, the respondent in writing dated 07/22/2021 has indicated that: “Regarding

tion to the minutes of the Citizen Council, in which the name of the claimant appears,

It should be noted that the publication of the minutes is an exercise in transparency of the public and

that in no case can it be understood that there is an affectation to honor or integration

morality of the claimant and much less an attack on his dignity, nor detriment to his rights.

fundamental guys.

In the future, this council, which will continue in its exercise of transparency,

will omit any name that may offend sensitivities.”

And later in a letter dated 03/08/2022, he pointed out the same issue

that “Certainly a minute of the citizen council was published on Facebook for the sake of

transparency of public actions. In said record there was information

with names and surnames that, in no case affects dignity or reveals any se-

secret, since what is published is public and notorious, nor can it be considered harmful to the interested parties.

ses or to the honor of anyone.

Furthermore, when the person in charge of the Diputación de Palencia

for data protection requested this town hall to withdraw the data to which

we mean, it was withdrawn immediately.”

However, it is estimated that the defendant would be responsible for the violation of the

article 5.1.f) of the RGPD, infringement typified in article 83.5.a) of the aforementioned regulation-

ment.

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

costs for treatment, including the conditions for consent under the

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

Article 83 of the aforementioned RGPD.

IV

On the other hand, the LOPDGDD in its article 71, Violations, establishes that:

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

4, 5 and 6 of Article 83 of Regulation (EU) 2016/679, as well as those resulting

are contrary to this organic law”.

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

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

ticular, the following:

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

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

(…)”

Second, it should be noted that the security of personal data

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

v

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 pro-

variable probability and severity for the rights and freedoms of natural persons,

the person in charge and the person in charge of the treatment will apply technical and organizational measures

appropriate channels to guarantee a level of security appropriate to the risk, which in its

case include, among others:

a) pseudonymization and encryption of personal data;

b) the ability to guarantee the confidentiality, integrity, availability and re-

permanent silence of treatment systems and services;

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

promptly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the treatment

I lie.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

9/15

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

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

accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or unauthorized access

torized to such 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

feel article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee

warrant that any person acting under the authority of the person in charge or the person in charge

do and have access to personal data can only process said data following instructions

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 the article

83.4.a) of the aforementioned RGPD in the following terms:

SAW

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

with paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or, alternatively,

being from a company, of an amount equivalent to a maximum of 2% of the volume

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

greater amount:

a) the obligations of the person in charge and of the person in charge in accordance with the articles

8,11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "Infringements considered serious":

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

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

following:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance

to what is required by article 32.1 of Regulation (EU) 2016/679".

(…)"

The GDPR defines personal data security breaches as “all

all those security violations that cause the destruction, loss or alteration

accidental or illicit ration of personal data transmitted, conserved or processed in

otherwise, or unauthorized communication or access to such data”.

The documentation in the file offers indications that the claimant

has violated article 32 of the RGPD, when a security incident occurred when

enable access to the administrative file in which a work of

claimant-driven construction; the third, a member of the Citizen Council

of the municipality, stated at a meeting of the aforementioned Council and that it was later uploaded to

Facebook, that the claimant had to adhere to the dispositions in the execution of his project.

put in the memory presented and approved by the local entity, without existing in the

Registration of the institution requesting access, which may imply an infringement of the

measures

organizational.

techniques

Y

It should be noted that the RGPD does not establish a list of security measures.

authority that are applicable according to the data being processed,

but it establishes that the person in charge and the person in charge of the treatment will apply measures

technical and organizational measures that are appropriate to the risk involved in the treatment,

taking into account the state of the art, the application costs, the nature, al-

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 the technical and

Organizational activities 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

you give.

In any case, when evaluating the adequacy of the security level, parti-

taking into account the risks presented by the processing of data, as a consequence

accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or unauthorized access

authorized to said data and that could cause physical, material and

them or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the processing from violating the

established in 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 art and the cost of its application with respect to

regarding the risks and the nature of the personal data to be protected. To the

assess the risk in relation to data security, should be taken into account

the risks arising from the processing of personal data, such as the destruction

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

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

data, susceptible in particular to cause physical, material or

immaterial".

It appears in the facts and in the framework of the file of previous investigations,

that the AEPD transferred the claim presented to the defendant so that he proceeded to

its analysis and report on the incident and the actions carried out, indicating in

writing of 07/22/2021 that the third party, member of the Citizen Council, to whom

re the claimant has never had access to the administrative file.

In writing of allegations to the agreement to initiate the sanctioning procedure

of 03/09/2022, the respondent reiterates and insists on his statements stating that

"This City Council, as it already indicated in its day, has never given access to any experience.

tooth to anyone who has not requested it through the regulatory channel. In the case that

we are dealing with, the member of the aforementioned citizen council has never requested the file

mentioned and has never had access to it."

It is true that the respondent has reported on the procedure implemented for

registration and consultation of the information and documentation contained in the administrative files

ministrative, providing a copy of the accesses made to the file from the

02/06/1019 to 08/25/2021, deducing that they were carried out by

claimed staff with authorized access; Furthermore, it should be noted that all

all workers have signed a confidentiality agreement and the

copy of the risk analysis report where the treatment "Administrative management" appears.

treatment of urban discipline files”.

However, it is also true that in the response offered to the AEPD also

It also pointed out that: “There are no records of access to files in pa-

role on the part of the corporation or public employees”, so it could be done

spoiled.

see

caused

access

a

No

In this sense, the responsibility of the claimed party is determined by the

security breach revealed, since it is responsible for making decisions

tions 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 and prevent access to them.

Therefore, in accordance with the foregoing, it is estimated that the respondent

would be allegedly responsible for the violation of article 32.1 of the RGPD, violation

typified in article 83.4.a).

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

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

viii

"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

tions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

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

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

d) Public bodies and public law entities linked to or de-

pending from 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 Legislative Assemblies

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

them.

2. When the persons in charge or persons in charge listed in section 1

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

organic, the data protection authority that is competent will issue resolutions

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

as the measures that should be adopted to stop the behavior or correct the effects

cough 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

gain of which it depends hierarchically, in his case, and to those affected who had the

Interested party status, if any.

3. Without prejudice to the provisions of the preceding section, the protection authority

tion of data will also propose the initiation of disciplinary actions when

there are sufficient indications for it. In this case, the procedure and the sanctions to

apply will be those established in the legislation on the disciplinary or sanctioning system.

dor 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 corresponding Official State or Autonomous Gazette.

gives.

4. The resolutions must be communicated to the data protection authority.

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

previous two paragraphs.

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

tions 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

ferred 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 infringement

tion.

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, the present sanctioning procedure comes

motivated based on the presumption that the respondent would have incurred in violation

of the regulations on data protection, articles 5.1.f) and 32.1 of the RGPD.

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

warning in relation to the processing of personal data that is not appropriate

Cuen to your forecasts. In this regard, article 83.7 of the RGPD contemplates that "Without

prejudice to the corrective powers of the supervisory authorities under article

58, paragraph 2, each Member State may establish rules on whether it can, and

To what extent, impose administrative fines on authorities and public bodies

established in that Member State.

In this same sense, article 58 of the RGPD, in its section 2 d) indicates

that each control authority may “order the person responsible or in charge of the treatment

I guarantee that the treatment operations comply with the provisions of this

Regulation, where appropriate, in a certain way and within a specified period.

cified…”.

As indicated previously, it has been proven that the defendant

has breached the data protection regulations, articles 5.1.f) and 32.1 of the RGPD, by

publish on facebook the personal data of the claimant and enable the

access to the administrative file, violating the technical and organizational measures.

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

the appropriate measures as indicated in articles 5.1.f) and 32.1 of the RGPD or

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

this procedure, as well as not informing this AEPD of the measures adopted

could give rise to the exercise of possible actions before the person in charge of the

treatment in order to effectively apply the appropriate measures to

guarantee and not compromise the confidentiality of personal data and the

right to personal privacy.

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

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the CITY COUNCIL OF SALINAS DE PISUERGA, with NIF

P3415800F, for an infringement of article 5.1.f) of the RGPD, typified in article

83.5.a) of the RGPD, a sanction of warning.

SECOND: IMPOSE the CITY COUNCIL OF SALINAS DE PISUERGA, with NIF

P3415800F, for an infringement of article 32.1 of the RGPD, typified in article

83.4.a) of the RGPD, a sanction of warning

THIRD: REQUEST the CITY COUNCIL OF SALINAS DE PISUERGA, so that

Within one month from the notification of this resolution, prove the adoption of

necessary and relevant technical and organizational measures in accordance with the

regulations regarding the protection of personal data in order to prevent

incidents such as those that have given rise to the

claim correcting the effects of its possible infraction, adapting the treatment

of personal data to the requirements contemplated in articles 5.1.f)

and 32.1 of the GDPR.

FOURTH: NOTIFY this resolution to the CITY COUNCIL OF SALINAS DE

PISUERGA.

FIFTH: COMMUNICATE this resolution to the Ombudsman, in accordance

with the provisions of article 77.5 of the LOPDGDD.

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

Electronic Registration of

through the

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.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es