Procedure No.: PS/00064/2021

 RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the claimant) on 08/22/2019 filed

claim before the Spanish Data Protection Agency. The claim is

directed against EL ESPINAR CITY COUNCIL with NIF P4008700I (hereinafter, the

reclaimed). The reasons on which the claim is based are the publication, through

side, of the lists of the components of the electoral tables with indication of

name and surnames, full address and ID.

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

Data Inspection proceeded to carry out the following actions:

On 11/28/2019, reiterated on 11/08/2019, the claim was transferred to the defendant

submitted for analysis and communication to the claimant of the decision adopted

regard. Likewise, it was required that within a month he send to the

Agency certain 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.

THIRD: On 06/08/2020, 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 by the claimant against the respondent.

FOURTH: The respondent did not respond in time to any of the requirements

indicated in the second fact carried out by the AEPD, although on 06/16/2020,

A letter was received from the respondent responding to the questions raised, indicating

that in the extraordinary plenary session of 04/29/2019, for the draw for the composition of the

polling stations related to the municipal elections of 05/26/201, the

data protection regulations without the attendees, except the councillors, being able to

have access to the confidential information of neighbors; that for the draw

used the computer program "ACCEDE" offered by the Diputación de Segovia and

that, in addition, these plenary sessions, unlike the rest, are not recorded,

stating in the minutes only the name of those designated by lottery and the position in

the polling station; that the claimed party has the Bandomovil service with the aim

to keep the residents of the municipality informed instantly of the news and

news of your interest and enforce the principle of information transparency

and that, in order to provide the residents of the municipality with the result of the lottery

concerning the composition of polling stations, published an extract of the headlines

and alternates, regardless of the subsequent personal notification to the designees;

however, on this occasion, it was published initially, as indicated by

the complainant the list that is automatically downloaded from the computer program

“ACCESS”; that said error is justified by the fact that the Local Police was the
responsible for carrying out the personal notifications to the designated and there was in
error with the lists and that at the time this incident was recorded,
deleted automatically to proceed later to upload the correct document.
Likewise, the respondent points out that on 11/16/2020 a Circular was issued with the
purpose of communicating to the staff the measures to be adopted in relation to the
notifications regarding data protection and that a review is being carried out
review and update on this matter in the City Council as a whole, with the
in order to avoid future security breaches of personal data.
FIFTH: On 02/18/2021, the Director of the Spanish Agency for the Protection of
Data agreed to initiate a sanctioning procedure against the defendant, for the alleged
infringement of articles 5.1.f) and 32.1 of the RGPD, sanctioned in accordance with the
provided in article 83.5.a) and 83.4.a) of the aforementioned RGPD, considering that the
sanction that could correspond would be a WARNING.
SIXTH: 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.
SEVENTH: Of the actions carried out in this procedure, they have been
accredited the following:
PROVEN FACTS
FIRST: On 08/22/2019 there is an entry in the AEPD written by the claimant

stating that the respondent has published, through an edict, the lists of

components of the electoral tables with indication of name and surnames, address

Complete and ID.

SECOND: The respondent in writing dated 06/16/2020 has stated that “he has the

Bandomovil service with the aim of keeping users informed instantly

neighbors of the municipality of the novelties and news of interest and make effective the

principle of transparency of municipal information.

… that, in order to provide the residents of the municipality with the result of the lottery related to the

composition of the polling stations, the City Council published an extract of the

holders and alternates, regardless of the subsequent personal notification to the

designated.

On this occasion, it was published initially, as indicated by the

complainant the list that is automatically downloaded from the computer program

"ACCESS" ... This error is justified by the fact that the Local Police was the

in charge of carrying out the personal notifications to the designated ones and there was a

error with lists.

(…)

Corrected the error, the new document was published in the Bandomovil service

in accordance with the provisions of Organic Law 3/2018, of December 5, of

Protection of Personal Data and guarantee of digital rights…”

FOUNDATIONS OF LAW

Yo

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

control authority, and as established in art. 47 of the Organic Law 3/2018, of

December 5, Protection of Personal Data and guarantee of rights

(hereinafter LOPDGDD), the Director of the Spanish Agency for

Data Protection is competent to resolve 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 facts denounced materialize in the publication, through the proclamation,

of the lists of the components of the electoral tables, violating the duty of

confidentiality.

III

Article 5, Principles relating to processing, of the GDPR states that:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized processing or

against its loss, destruction or accidental damage, through the application

of appropriate technical or organizational measures ("integrity and

confidentiality").

(…)

Also article 5, Duty of confidentiality, of the new Organic Law

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

digital rights (hereinafter LOPDGDD), states that:

"1. Those responsible and in charge of data processing as well as all

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

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

of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain

even when the relationship of the obligor with the person in charge or person in charge had ended

of the treatment".

On the other hand, article 83.5 a) of the RGPD, considers that the infringement of "the

basic principles for processing, including conditions for consent

IV

in accordance with articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the mentioned article 83 of the aforementioned GDPR, "with administrative fines of €20,000,000 maximum or, in the case of a company, an amount equivalent to 4% as maximum of the overall annual total turnover of the previous financial year, opting for the highest amount.

The LOPDGDD in its article 72 indicates: "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:

a) The processing of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679.

(…)

v

The documentation in the file shows that the defendant violated article 5 of the RGPD, principles related to the treatment, in relation to the Article 5 of the LOPGDD, duty of confidentiality, when published through side, the lists of the components of the electoral tables of the elections of 05/26/2019 with indication of personal data, violating the principle of data confidentiality.

This duty of confidentiality, previously the duty of secrecy, must understood that its purpose is to prevent leaks of data not consented to by their owners.

Therefore, this duty of confidentiality is an obligation that falls not only to the person in charge and in charge of the treatment but to everyone who intervenes in

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

Second, article 32 of the RGPD “Security of treatment”,

SAW

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 the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the

treatment.

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

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

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

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 controller or the

manager and has access to personal data can only process said data

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

Law of the Union or of the Member States".

The violation of article 32 of the RGPD is typified in the article

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

7th

"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,

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 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:

(…)

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 facts revealed in this claim materialize

in the publication, through bando, of the lists of the components of the tables

electoral documents indicating name and surname, full address and DNI, with

breach of technical and organizational measures.

The GDPR defines personal data security breaches as

"all those violations of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

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

viii

From the documentation in the file, there are clear indications of

that the claimed party has violated article 32 of the RGPD, when an incident of

security with the publication, through bando, of the lists of the components of

polling stations allowing access to personal data with

breach of technical measures.

It should be noted that the RGPD in the aforementioned provision does not establish a list of the security measures that are applicable according to the data that is object of treatment, but it establishes that the person in charge and the person in charge of the treatment will apply technical and organizational measures that are appropriate to the risk that the treatment entails, taking into account the state of the art, the costs of application, the nature, scope, context and purposes of the treatment, the risks of probability and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate to the detected risk, pointing out that the determination of the measures technical and organizational information must be carried out taking into account: pseudonymization and encryption, the ability to ensure the confidentiality, integrity, availability and resiliency, the ability to restore availability and access to data after a incident, verification process (not audit), evaluation and assessment of the effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security, particularly taking into account the risks presented by the processing of data, such as consequence of the accidental or unlawful destruction, loss or alteration of data data transmitted, stored or otherwise processed, or the communication or unauthorized access to said data and that could cause damages physical, material or immaterial.

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

"(83) In order to maintain security and prevent the treatment from violating the provided 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

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

In the present case, as evidenced by the facts and within the framework of the

investigation file E/09597/2019 the AEPD transferred the defendant on

11/28/2019, reiterated on 11/08/2019, the claim submitted for analysis

requesting the provision of information related to the incident produced, without

that no reply had been received within the time limit. However, after the

Over the course of the indicated periods, a response was sent confirming the

claimed incidence, although measures had been adopted with the aim of avoiding

future security breaches of personal data.

The responsibility of the claimed party is determined by the bankruptcy of

security revealed by the claimant, since it is responsible for taking

decisions aimed at effectively implementing technical measures and

appropriate organizational measures to guarantee a level of security appropriate to the risk

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

access to them in the event of a physical or technical incident. However, from the

The documentation provided shows that the entity has not only breached this obligation, but also the adoption of measures in this regard is unknown, despite of having notified him of the claim filed.

In accordance with the foregoing, it is estimated that the respondent would be allegedly responsible for the violation of article 32 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:

IX

"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.

The sanctioning procedure brings cause of the publication of the data of the

lists of the components of the electoral tables of the elections of 05/26/2019, to

through bando, infringing the data protection regulations of

personal nature, considering that it violates both the principle of confidentiality and

as well as the technical and organizational measures implemented.

Said conduct constitutes, on the part of the defendant, the infraction of the provisions

in articles 5.1.f) and 32.1 of the RGPD.

It should be noted that 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.

Likewise, it is contemplated that the resolution may establish the measures

that it is appropriate to adopt so that the conduct ceases, the effects of the infraction are corrected

that had been committed, the adequacy of the processing of personal data

personnel to the requirements contemplated in articles 5.1.f) and 32.1 of the RGPD, as well

as the provision of means accrediting compliance with what is required.

However, the respondent in his response to this body dated

06/16/2020 confirmed the publication at first, as indicated by the

claimant, from the list of components of the electoral tables of the elections of

05/26/2019, although at the time this fact was recorded,

proceeded to automatically delete and subsequently upload the correct document, without

that there is a trace of the erroneous document; corrected the error was published in the service

Bandomovil the new document in accordance with the provisions of the

LOPDGDD. Subsequently, on 12/16/2020, a Circular was issued in order to

communicate to the City Council staff the measures to be adopted in relation to the

notifications on data protection and that in this matter is being

proceeding to a review and update in the whole of the Corporation with the

objective of avoiding future breaches of data security and confidentiality

personal.

In light of the foregoing, it is not appropriate to urge the adoption of measures

additional, having been proven that the respondent has adopted measures

reasonable and appropriate measures to prevent the recurrence of incidents such as the one

gave rise to the claim in accordance with the regulations on protection

of data, main purpose of the procedures with respect to those entities

listed in article 77 of the LOPDGDD.

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 EL ESPINAR, with NIF P4008700I, by

an infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the RGPD,

a sanction of warning in accordance with article 77 of the LOPDGDD.

SECOND: IMPOSE THE CITY COUNCIL OF EL ESPINAR, with NIF P4008700I, for

an infringement of article 5.1.f) of the RGPD, typified in article 83.5.a) of the RGPD,

a sanction of warning in accordance with article 77 of the LOPDGDD.

THIRD: NOTIFY this resolution to the CITY COUNCIL OF EL ESPINAR.

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