 File No.: EXP202104939

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), on October 16,

2021, filed a claim with the Spanish Data Protection Agency. The

claim is directed against the CITY COUNCIL OF LAS PALMAS DE GRAN

CANARIA, with NIF P3501700C (hereinafter, the claimed party). The reasons in which

the claim is based on are as follows:

The claimant states that, on the website of the CITY COUNCIL OF LAS PALMAS

OF GRAN CANARIA, the minutes of the Plenary Session, dated

01/28/2019, where it is recorded, in relation to some allegations made to a

municipal ordinance, your name, surnames and DNI.

Along with the claim, provide the minutes.

It has been found that the aforementioned document is currently accessible,

displaying controversial data.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the claimed party,

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

data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

(hereinafter, LPACAP) by electronic notification, was not collected by

the person in charge, within the period of making available, understanding rejected,

in accordance with the provisions of art. 43.2 of the LPACAP, dated December 10,

2021, as stated in the certificate that is in the file.

Although the notification was validly made by electronic means, assuming

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, by way of

informative, a copy was sent by mail that was reliably notified in

dated December 20, 2021. In said notification, he was reminded of his obligation to

communicate electronically with the Administration, and they were informed of the means

of access to said notifications, reiterating that, in the future, you would be notified

exclusively by electronic means.

No response has been received to this transfer letter.

THIRD: On January 16, 2022, in accordance with article 65 of the

LOPDGDD, the admission for processing of the claim presented by the

claiming party.

FOURTH: On June 24, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimed party,

for the alleged infringement of articles 5.1.f) and 32 of the RGPD, typified in the

articles 83.5 and 83.4 of the RGPD, respectively.

The initiation agreement was sent, in accordance with the regulations established in the Law

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

Public Administrations (hereinafter, LPACAP), by electronic notification,

being received on June 28, 2022, as stated in the certificate that works

on the record.

FIFTH: Notification of the aforementioned start-up agreement in accordance with the rules established in

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

Public Administrations (hereinafter, LPACAP) and after the term granted

for the formulation of allegations, it has been verified that no allegation has been received

any by the claimed party.

Article 64.2.f) of the LPACAP - provision of which the respondent was informed

in the agreement to open the procedure - establishes that if no

allegations within the stipulated period on the content of the initiation agreement, when

it contains a precise statement about the imputed responsibility,

may be considered a resolution proposal. In the present case, the agreement

beginning of the sanctioning file determined the facts in which the

imputation, the infraction of the RGPD attributed to the claimed and the sanction that could

prevail. Therefore, taking into consideration that the respondent has not

formulated allegations to the agreement to initiate the file and in attention to what

established in article 64.2.f) of the LPACAP, the aforementioned initial agreement is

considered in this case proposed resolution.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It is recorded that on October 16, 2021, the complaining party filed

claim before the Spanish Agency for Data Protection, against the

CITY COUNCIL OF LAS PALMAS DE GRAN CANARIA, having published in its

website, the minutes of the Plenary Session dated 01/31/2019, where it is recorded in

regarding allegations you made to a municipal ordinance, your name,

surnames and ID.

SECOND: It has been verified that the document is accessible on the web

of the said body.

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

control authority and as established in articles 47 and 48.1 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

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

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

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures.”

II

Local Regime Legislation

Regarding publicity of municipal activities, article 70 of the Law

Regulator of the Bases of the Local Regime, (LBRL), in the wording given to it

by Law 57/2003, of 16/12, provides the following:

"1. The plenary sessions of the local corporations are public. Nope

However, the debate and vote on those matters that

may affect the fundamental right of citizens referred to in

Article 18.1 of the Constitution, when so agreed by an absolute majority.

The sessions of the Local Government Board are not public.

2. The agreements adopted by the local corporations are published or notified

in the manner provided by law.

3. All citizens have the right to obtain copies and certifications

accrediting the agreements of local corporations and their background,

as well as to consult the files and records in the terms provided by the

implementing legislation of article 105, paragraph b), of the Constitution. The

denial or limitation of this right, in everything that affects the security and

defense of the State, the investigation of crimes or the privacy of individuals

must be verified by reasoned resolution."

That the sessions are not public does not add anything about the publication of the acts

administrative, since they govern general rules on notification and publicity of the

agreements as appropriate (art. 70.2 LBRL).

The regulation referred to by the LBRL can be found in its development rule, the

Royal Decree 2568/1986, of 11/28, which approves the Regulation of

Organization, Operation and Legal Regime of Local Entities.

"Article 229

1. The calls and agendas of the plenary sessions will be transmitted

to the social media of the locality and will be made public in the

Notice board of the entity.

2. Without prejudice to the provisions of article 70.2 of Law 7/1985, of April 2,

The Corporation will give summarized publicity of the content of the plenary sessions

and of all the agreements of the Plenary and of the Government Commission, as well as of

the resolutions of the mayor and those dictated by his delegation by the Delegates."

Nothing is specified on the minutes, nor on the minutes of the Local Government Board. Of

In the same way, the basic principles of data protection link the minimization

of data, adequacy and need for treatment with the purpose in article 5.1 c)

"Principles relating to processing":

1. The personal data will be:

c) adequate, relevant and limited to what is necessary in relation to the purposes

for which they are processed ("data minimization");

Not specifying what should be the summary that can be published of the sessions

plenary sessions, and not making express reference to the publication of the minutes of the Board of

Local Government, there is no legal mandate for said summary to offer the same

content that article 109 prevents for the minutes, and therefore, the part

dispositive of the agreements that are adopted, and on the other, the essential nucleus of the right

of information of the neighbors remains intact insofar as they always and

regardless of the publication of said abstract, they may directly exercise

the right to information.

The "summary" referred to in said precept recommends eliminating from the same

those personal data that are not adequate, pertinent and are

excessive in order to offer "generic" information to the neighbors, and from

then in no case should they contain sensitive personal data.

Otherwise, this minimization duty is specified in the additional provision

seventh of the LOPDGDD, which establishes the following:

“When the affected party lacks any of the documents mentioned in the

two preceding paragraphs, the affected party will be identified only by name and

surnames. In no case should the name and surnames be published together

with the complete number of the national identity document, identity number of

foreigner, passport or equivalent document.

III

Previous issues

The City Council of Las Palmas de Gran Canaria, like any other public entity,

is obliged to comply with Regulation (EU) 2016/679 of the European Parliament

and of the Council of April 27, 2016, regarding the protection of natural persons

regarding the processing of personal data and the free circulation of these

data -RGPD-, and of the LO 3/2018, of December 5, of Protection of Personal Data-

them and Guarantee of Digital Rights -LOPDGDD- with respect to the treatments

of personal data that they carry out, understanding by personal data

nal, “all information about an identified or identifiable natural person”. It is considered

An identifiable natural person is one whose identity can be determined, directly or

indirectly, in particular by means of an identifier, such as a name,

an identification number, location data, an online identifier, or one or more

various elements of physical, physiological, genetic, psychic, economic identity,

cultural or social heritage of that person.

Likewise, treatment should be understood as “any operation or set of operations

tions made on personal data or sets of personal data, either by

automated procedures or not, such as the collection, registration, organization, structure

ration, conservation, adaptation or modification, extraction, consultation, use, co-

communication by transmission, broadcast or any other form of authorization of access,

collation or interconnection, limitation, suppression or destruction”.

Taking into account the above, (…).

It carries out this activity in its capacity as data controller, since it is

who determines the purposes and means of such activity, by virtue of article 4.7 of the RGPD:

“responsible for the treatment” or “responsible”: the natural or legal person, authority

public, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

determines the purposes and means of the treatment, the person responsible for the treatment or the criteria

specific for their appointment may be established by the Law of the Union or of the

Member states.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of se-

security of personal data” (hereinafter security breach) as “all

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

accidental or unlawful transfer of personal data transmitted, stored or processed in

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

In the present case, there is a security breach of personal data in the

circumstances indicated above, categorized as a breach of confidentiality,

whenever the City Council has revealed information and personal data to

third parties, without the express consent of the owner of said data, when publishing in their

website the minutes of the Plenary Session dated 01/31/2019, where the

name, surnames and ID of the claimant.

This type of data, as well as any other information that is referred to

natural persons, are considered personal data, so their

Treatment is subject to data protection regulations and since there is no

a legal obligation of the City Council to carry out such publication, it is necessary to

consent of the affected party to proceed with the aforementioned publication.

According to GT29, a "Breach of confidentiality" occurs when there is

unauthorized or accidental disclosure of personal data, or access to

themselves.

It should be noted that the identification of a security breach does not imply the imposition

sanction directly by this Agency, since it is necessary to analyze the

diligence of those responsible and in charge and the security measures applied.

Within the principles of treatment provided for in article 5 of the RGPD, the

integrity and confidentiality of personal data is guaranteed in section 1.f)

of article 5 of the RGPD. For its part, the security of personal data comes

regulated in articles 32, 33 and 34 of the RGPD, which regulate the security of the

treatment, notification of a violation of the security of personal data to

the control authority, as well as the communication to the interested party, respectively.

IV

Article 5.1.f) of the RGPD

Article 5.1.f) of the RGPD establishes the following:

“Article 5 Principles relating to processing:

1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

its loss, destruction or accidental damage, through the application of technical measures

or appropriate organizational structures (“integrity and confidentiality”).”

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the RGPD, principles related to treatment.

The AEPD verifies that, at least up to the present date, it is possible to access the

content of the Act by typing the electronic address of the City Council in the

browser, so the publication on the data web page is accredited

personal data of the claimant, such as their name, surnames and DNI.

Consequently, it is considered that the proven facts are constitutive of

infringement, attributable to the claimed party, for violation of article 5.1.f) of the

GDPR.

Classification of the infringement of article 5.1.f) of the RGPD

v

The aforementioned infringement of article 5.1.f) of the RGPD supposes the commission of the infringements typified in article 83.5 of the RGPD that under the heading “General conditions for the imposition of administrative fines” provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the global total annual turnover of the previous financial year, opting for the largest amount:

a) the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes that

“The acts and behaviors referred to in sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result contrary to this organic law.

For the purposes of the limitation period, article 72 “Infringements considered very serious” of the LOPDGDD indicates:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679, considered very serious and will prescribe after three years the infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

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

SAW

Article 32 of the GDPR

Article 32 of the RGPD, security of treatment, establishes the following:

"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 account shall be taken of

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

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

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

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a certification mechanism approved under article 42 may serve as an element to demonstrate compliance with the requirements established in section 1 of the present article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that any person acting under the authority of the person in charge or the person in charge and has access to personal data can only process said data following instructions of the person in charge, unless it is obliged to do so by virtue of the Right of the Union or the Member States.

The facts revealed imply the lack of technical measures and organizational by enabling the display of personal data of the claimant with the consequent lack of diligence by the person in charge, allowing access not authorized by third parties.

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

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

measures.

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

particularly taking into account the risks presented by the processing of data, such as

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

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

unauthorized access to said data and that could cause damages

physical, material or immaterial.

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

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

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.

The responsibility of the claimed party is determined by the lack of preventive measures.

security, since it is responsible for making decisions aimed at implementing

effectively the appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk to ensure the confidentiality of the data,

restoring their availability and preventing access to them in the event of an incident

physical or technical.

Therefore, the proven facts constitute an infraction, attributable to the

claimed party, for violation of article 32 RGPD.

Classification of the infringement of article 32 of the RGPD

7th

The aforementioned infringement of article 32 of the RGPD supposes the commission of the infringements

typified in article 83.4 of the RGPD that under the heading "General conditions

for the imposition of administrative fines" provides:

"The infractions of the following dispositions will be sanctioned, in accordance with the

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

in the case of a company, an amount equivalent to a maximum of 2% of the

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

the largest amount:

a)

the obligations of the person in charge and the person in charge in accordance with articles 8,

11, 25 to 39, 42 and 43; (…)"

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes that

"The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

For the purposes of the limitation period, article 73 "Infringements considered serious"

of the LOPDGDD indicates:

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

considered serious and will prescribe after two years the infractions that suppose a

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

following:

f) The lack of adoption of those technical and organizational measures that

are appropriate to guarantee an adequate level of security when

risk of treatment, in the terms required by article 32.1 of the

Regulation (EU) 2016/679.”

viii

Responsibility

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III on the "Principles of the power to impose penalties", in article 28

under the heading “Responsibility”, the following:

"1. They may only be sanctioned for acts constituting an administrative infraction.

natural and legal persons, as well as, when a Law recognizes their capacity to

to act, the affected groups, the unions and entities without legal personality and the

independent or autonomous estates, which are responsible for them

title of fraud or guilt.”

Lack of diligence in implementing appropriate security measures

with the consequence of breaching the principle of confidentiality constitutes the

element of guilt.

IX

Sanction

Article 83 “General conditions for the imposition of administrative fines” of the

RGPD in its section 7 establishes:

“Without prejudice to the corrective powers of the control authorities under the

Article 58(2), each Member State may lay down rules on whether

can, and to what extent, impose administrative fines on authorities and organizations

public authorities established in that Member State.”

Likewise, article 77 “Regime applicable to certain categories of

responsible or in charge of the treatment” of the LOPDGDD provides the following:

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

who are responsible or in charge:

(…)

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

autonomous and the entities that make up the Local Administration.

2. When those responsible or in charge listed in section 1 committed

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

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

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

the effects of the infraction that had been committed.

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

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

interested party, if any.

(…)

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

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

under this article."

In the present case, it is considered appropriate to sanction the party with a warning.

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

of the RGPD, due to the lack of diligence in implementing the appropriate measures

with the consequence of breaking the principle of confidentiality.

X

Measures

Article 58.2 of the RGPD provides: "Each control authority will have all the

following corrective powers indicated below:

d) order the person in charge or in charge of the treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate,

in a specified manner and within a specified period;”

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the

RGPD and order the claimed party to, within a month, establish the measures

adequate security measures so that the treatments are adapted to the demands

contemplated in articles 5.1 f) and 32 of the RGPD, preventing the occurrence of si-

similar situations in the future.

The text of the resolution establishes the infractions committed and

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

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

that the type of specific procedures, mechanisms or instruments for

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

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

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

LOPDGDD.

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

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: SANCTION the CITY COUNCIL OF THE

PALMAS DE GRAN CANARIA, with NIF P3501700C, for an infringement of article

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

SECOND: TO SANCTION the CITY COUNCIL OF THE

PALMAS DE GRAN CANARIA, with NIF P3501700C, for an infringement of article 32

of the RGPD, typified in article 83.4 of the RGPD.

THIRD: REQUEST the CITY COUNCIL OF LAS PALMAS DE GRAN CANARIA,

to implement, within a period of one month, the necessary corrective measures to adapt

their performance to the personal data protection regulations, which prevent the

similar events are repeated in the future, as well as to inform this Agency in the same

term on the measures adopted.

FOURTH: NOTIFY this resolution to the CITY COUNCIL OF LAS PALMAS

OF GRAN CANARIA.

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, this

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

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

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

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

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

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

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

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

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

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

aforementioned Law.

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

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-120722

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es