 Procedure No.: PS/00144/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following:

BACKGROUND

FIRST: Don A.A.A. (hereinafter, the claimant), dated December 18,

2019, filed a claim with the Spanish Data Protection Agency. The

claim is directed against the CITY COUNCIL OF ***CITY COUNCIL.1 with CIF

P3502000G (hereinafter the claimed one).

The reasons on which he bases his claim are, in short: that he filed a

demand for claim of amount against the claimed and indicates that, a

worker of this, has sent the sentence to several workers through WhatsApp

of the aforementioned judicial procedure in which your personal data is recorded. I know

Provides screen printing of the mobile terminal with a WhatsApp message on the

which is informed of the distribution of the sentence.

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), the claim was transferred on February 18, 2020.

information to the claimant, so that he could proceed with his analysis and inform this Agency in

within a month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

The request for information was delivered on February 24, 2020, without

that a reply was received.

THIRD: On August 6, 2020, the Director of the Spanish Agency for

Data Protection agreed to formally admit the claim submitted for processing

by the claimant, in accordance with article 65 of the LOPDGDD.

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

of previous investigative actions to clarify the facts

of the claim, having knowledge of the following extremes:

- Notified to the respondent, dated September 11, 2020, request for

information on the facts claimed and the legitimacy of access to this type of

documents by the person who sent the WhatsApp message with the document

sentence, after four months this Agency has not received a letter of

allegations forwarded by the respondent.

- This request is reiterated, with a notification date of January 25, 2021, no

Respondent's response has been received.

FIFTH: On April 16, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, for the

alleged infringement of Article 32 of the RGPD, Article 5.1.f) of the RGPD, typified in the

Article 83.5 of the RGPD.

SIXTH: The initiation agreement was electronically notified to the respondent. so demands it

Article 14.2 of Law 39/2015 on Common Administrative Procedure of the Administrations

Public Administrations (LPACAP) according to which "In any case they will be obliged to

interact through electronic means with the Public Administrations for the

carrying out any procedure of an administrative procedure, at least, the following

following subjects: a) Legal persons".

Works in the file the Certificate issued by the Notification Service
Electronic and Authorized Electronic Address of the FNMT-RCM, which records
the sending of the initiation agreement, notification of the AEPD addressed to the claimed, through
through that means being the date of availability in the electronic headquarters of the
agency on April 16, 2021 and the automatic rejection date on April 27,
2021.

SEVENTH: In accordance with article 73.1 of the LPCAP, the term to formulate
allegations to the Home Agreement is ten days computed from the day following the
of the notification.

Article 64.2. LPACAP, indicates that the defendant will be informed of the right to
formulate allegations, the "right to be heard in the procedure and the deadlines
for its exercise, as well as the indication that in case of not making allegations in
the term established on the content of the initiation agreement, it may be considered
proposed resolution proposal when it contains a precise pronouncement about
the imputed responsibility". (The underlining is from the AEPD)

The agreement to initiate the sanctioning file that concerns us contained a pro-
precise statement on the responsibility of the claimed entity: in the aforementioned
agreement specified what was infringing conduct, the sanctioning type in which it was
subsumable, the circumstances of the responsibility described and the sanction that in the judgment
of the AEPD proceeded to impose.

In consideration of the foregoing and in accordance with the provisions of article
Article 64.2.f) of the LPACAP, the initiation agreement of PS/00106/2021 is considered Pro-
Resolution: Once the initiation agreement has been notified, the one claimed at the time of the
This resolution has not submitted a brief of arguments, so it is
application of what is stated in article 64 of Law 39/2015, of October 1, of the
Common Administrative Procedure of Public Administrations, which in its

section f) establishes that in the event of not making allegations within the stipulated period 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.

In view of everything that has been done, by the Spanish Data Protection Agency In this proceeding, the following are considered proven facts:

FACTS

FIRST: Mr. A.A.A., public employee on leave of absence from the CITY COUNCIL OF ***CITY COUNCIL.1 submitted a claim for the amount to that City Council.

SECOND: Sentence issued on the matter, a City Council worker en- He saw the sentence through WhatsApp to several workers. In the Judgment there are personal data of the claimant.

THIRD: It is accompanied by an image of a screen of a mobile phone in which a person indicates to the respondent that they have received the aforementioned Judgment.

FOURTH: The requested City Council has not responded to the information requirements information sent by the Data Inspection of the Spanish Agency for the Protection of Data relating to this claim, despite having received the electronic notification requesting information on dates January 24 and September 11, 2020, and January 2021. The initiation agreement notified in the same way as the requirements information, and yet it was expired.

FOUNDATIONS OF LAW

Yo

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

control, and as established in arts. 47 and 48.1 of the LOPDGDD, the Directorate

tora of the Spanish Agency for Data Protection is competent to resolve this

process.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of Regulation 2016/679 (EU) of

data protection (hereinafter RGPD) recognizes each control authority, and se-

According to what is established in articles 47 and 48.1 of Organic Law 3/2018, of 5

December, Data Protection and Guarantees of digital rights (LOPDGDD),

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

see this procedure.

II

The facts claimed are specified in a worker of the claimed sent to

through the social network WhatsApp to several workers of the consistory the sentence of the

judicial proceeding instituted by the claimant against the respondent in which the

your personal data.

The RGPD deals in its article 5 with the principles that must preside over the

treatment of personal data and mentions among them those of "integrity and

confidentiality". The provision provides:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing,

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

appropriate technical or organizational (<<integrity and confidentiality>>)".

Article 5.2. RGPD establishes: "The data controller will be

responsible for compliance with the provisions of paragraph 1 and capable of

demonstrate it (<<proactive responsibility>>)"

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of 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".

III

The documentation in the file, and which has not been distorted by

the claimed, proves that the claimed, violated article 5 of the RGPD, principles

related to treatment, in relation to article 5 of the LOPGDD, duty of confi-

confidentiality, by allowing the personal data of the claimant contained

in a judicial sentence were published, through the WhatsApp social network, by a

worker of the consistory referring to other workers violating the duty of

confidentiality.

This duty of confidentiality, previously the duty of secrecy, must be understood

It should be noted that its purpose is to prevent leaks of the data not being carried out.

felt 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.

IV

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, "with administrative fines of €20,000,000 maximum

or, in the case of a company, an amount equivalent to a maximum of 4% of the

global annual total business lumen of the previous financial year, opting for the

of greater amount”.

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

“Infringements considered very serious:

1. Based on the provisions of article 83.5 of 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.

(…)”

v

The principle of integrity established in article 5.1.f) RGPD is developed through

through articles 32 to 34 RGPD, framed in section II of chapter IV that

It bears the heading “Security of personal data”. Article 32, “Security of the

treatment," he says:

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

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

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

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

appropriate 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.

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 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. (…)

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 underlining is from the AEPD)

SAW

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

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

"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 the person in charge pursuant to articles 8,

11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 71, Violations, states that: "Consti-

The acts and behaviors referred to in sections 4, 5 and 6 are infractions

of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to

this organic law".

And in its article 73, for the purposes of prescription, it qualifies as "Infringements considered

serious cracks":

"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".

(…)"

7th

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".

From the documentation in the file, it is verified that the defendant,

through an employee of your organization, has violated article 32 of the RGPD, by

a security incident occurs in your system allowing access to third parties

personal data of another public employee, when displayed through the social network

social WhatsApp when a worker referred other workers of the consistory sent

court order requested by the claimant against the consistory allowing access to

your personal data with violation of technical measures and

organizational.

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 treatment entails, taking into account the state of the art, the costs of applying cation, 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 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”.

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

evidenced by the claimant, since he 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, restoring its availability and preventing access to the

in the event of a physical or technical incident. However, the entity has not only in-

fulfilled this obligation, but also transfers the claim so that it informs

to this Agency about the incidence produced and communicate about the decision adopted

in this regard, he ignored not answering anything.

In accordance with the foregoing, it is estimated that the respondent is responsible

ble of the infraction of the RGPD: the violation of article 32, infraction typified in its

article 83.4.a).

Regarding the statute of limitations for this infraction, we will have to be at the

provisions of the (LOPDGDD). Article 73, f) LOPDGDD qualifies as a serious infringement

"The lack of adoption of those technical and organizational measures that are appropriate

to guarantee a level of security appropriate to the risk of treatment in the

terms required by article 32.1 of Regulation (EU) 2016/679". Article 73

LOPDGDD provides that serious infractions will have a statute of limitations of

two years.

Article 83.7 of the RGPD affects the following:

viii

Without prejudice to the corrective powers of the control authorities under

of 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."

The Spanish legal system has chosen not to sanction with a fine those

public entities, as indicated in article 77 of the LOPDDGG, which establishes

ce the following:

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

who are responsible or in charge:

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.

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 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

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 present case, it has been proven that the aforementioned conduct constitutes

asserts, on the part of the defendant, the infringement of the provisions of article 5.1.f) and 32.1

of the GDPR.

Likewise, the measures to be adopted will be established to stop the

conduct, correct the effects of the infraction that had been committed and its ade-

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

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

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 ***CITY COUNCIL.1 with CIF

P3502000G, for a violation of article 5.1.f) of the RGPD, in accordance with the ar-

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

SECOND: IMPOSE the CITY COUNCIL OF ***CITY COUNCIL.1 with CIF

P3502000G, for an infringement of article 32 of the RGPD, in accordance with article

Article 83.5 b) of the RGPD, a penalty of warning.

THIRD: In accordance with article 58.2. d) of the RGPD, the controller is ordered

ble of the treatment that the treatment operations comply with the provisions

of this Regulation, and must inform this AEPD of its execution within the period

of one month.

FOURTH: NOTIFY this resolution to the CITY COUNCIL OF ***CITY COUNCIL-

LYING.1.

FIFTH

with the provisions of article 77.5 of the LOPDGDD.

: COMMUNICATE this resolution to the Ombudsman, in accordance

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

resents may optionally file an appeal for reconsideration before the Director

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

the day following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court,

in accordance with the provisions of article 25 and section 5 of the additional provision

Final fourth of Law 29/1998, of July 13, regulating the Contentious Jurisdiction-

administrative, within a period of two months from the day following the notification

tion of this act, as provided for 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 interested party

do states its intention to file a contentious-administrative appeal. Of being

In this case, the interested party must formally communicate this fact in writing

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

Electronic registry of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or to

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

that proves the effective filing of the contentious-administrative appeal. If the

Agency was not aware of the filing of the contentious-administrative appeal

tive within two months from the day following the notification of this

resolution, would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

938-131120

www.aepd.es

sedeagpd.gob.es

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es