 File No.: PS/00396/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the complaining party) dated November 20,

2020, filed a claim with the Spanish Data Protection Agency. The

claim is directed against the CITY COUNCIL OF SAN JAVIER with NIF

P3003500J (hereinafter, the CITY COUNCIL). The reasons on which the

claim are as follows:

The City Council of San Javier has published on its website the Minutes of the Board of

Government held on 10/21/20, and in it the data related to the

productivity supplement for workers identified by their name and

their last names.

Together with the claim, a screen print of the website of the

CITY COUNCIL and the controversial act. It is also stated that it was already declared

infraction of the City Council of San Javier for the same reason: publication of data

in the minutes of the Local Government Boards.

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 CITY COUNCIL, 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.

There is no record that the respondent has responded to the transfer made by the Agency

Spanish Data Protection.

THIRD: In accordance with article 65 of the LOPDGDD, dated 02/15/2021,

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

claim filed by the claimant.

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:

On November 20, 2020, the complaining party filed a claim

on the facts described (alleged violation of Article 5 of the RGPD).

On 02/12/2021, the AEPD received a letter of communication of the breach of

security with number O00007128e2100005749 sent by the City Council of San

Javier in relation to the publication on the website of the Minutes of the Governing Board of 27

October 2020.

RESULT OF THE INVESTIGATION ACTIONS

1.- On March 11, 2021, a response was received from the CITY COUNCIL and the

the following follows:

Regarding the defendant

 The City Council of San Javier has signed a contract to carry out

DPD functions with a third entity.

Regarding the chronology of events. Actions taken in order to minimize

adverse effects and measures adopted for their final resolution

 On October 21, 2020, the Local Government Meeting takes place. Both the Act

as the Extract of the same are exposed to the public between days 2 to 16

November 2020.

In this regard, they have provided the Minutes of the Governing Board containing a

list of employees with personal data and Extract in which they do not appear

employee personal data.

 On February 2, 2021, the CITY COUNCIL has proof of the transfer of the

claim filed with the AEPD regarding the publication of the Minutes, and on 9

February it is verified that the error occurred to send to public exposure

both the minutes and its extract, when the habitual and reiterated thing is only to expose

the extract.

 On February 12, 2021, the information gap was notified.

security to the AEPD.

 Between February 12 and February 19, those affected were determined, (…).

 On February 22 (…).

 On March 11, 2021, the DPD received a request from the AEPD

requesting information and on March 12 it was received in the register of the

City Hall the same request.

Regarding the affected data

 The data of: (...) have been affected by the publication.

 The CITY COUNCIL has provided a letter addressed to those affected, communicating

the gap.

 The CITY COUNCIL states that the claim filed by two

employees who were affected by the breach, it does not appear that they

suffered damage derived from said publication, nor did they allege possible

negative consequences due to the publication of such data, beyond the

own violation of the regulations by disclosing more information than is due in

the terms of this breach.

 The CITY COUNCIL states that there is no record of the use by

third parties of the personal data obtained through the breach.

The published record (...).

Regarding the security measures implemented

 The CITY COUNCIL states that no security measure has failed

and have operated correctly the access control mechanisms and

authentication. (...).

 The CITY COUNCIL states that materials are being prepared

audiovisual training (information pills) to raise awareness on

data protection for personnel, where good

concrete and concise practices and guidelines. (...).

Regarding notification after 72 hours

(…)

Information on the recurrence of these events and the number of similar events that occur

woven in time

 The City Council of San Javier was warned in a sanctioning procedure

processed by the AEPD (AP/00007/2013), due to events that occurred last

May 11, 2012, (…).

FIFTH: On September 1, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the CITY COUNCIL,

for the alleged infringement of Article 5.1.f) of the RGPD, typified in Article 83.5 of the

RGPD, Article 32 of the RGPD, typified in Article 83.4 of the RGPD and Article 33 of the

RGPD, typified in Article 83.4 of the RGPD.

SIXTH: On October 4, 2021, a resolution proposal was formulated,

proposing that, due to the infringement of articles 5.1.f), 32 and 33 of the RGPD, typified

respectively in articles 83.5 and 83.4 of the RGPD, the Director of the Agency

Spanish Data Protection Agency directs a WARNING to the CITY COUNCIL OF

SAN JAVIER, with NIF P3003500J.

SEVENTH: On October 22, 2021, the CITY HALL presents a new

pleadings brief.

PROVEN FACTS

FIRST: It is proven that the City Council of San Javier has published in its

website the Minutes of the Governing Board held on 10/21/20, and it contains

publish the data related to the complement of productivity of the workers

identified by their first and last names. Along with the claim is provided

screen print of the website of the CITY COUNCIL and the controversial act.

SECOND: It is proven that the data has been affected by the publication

of: name and surname, position, productivity supplements and overtime of 126

employees.

THIRD: There is no evidence of the use by third parties of the data

personal gains through the breach.

FOURTH: The published record was not indexed on the web, so that it could only be

access it if the path or URL was known. Therefore, it was not possible to access the

itself by entering in the browser or indexer identifying data of the

affected stakeholders.

FIFTH: It is proven that, according to the CITY COUNCIL, advertising

of the data was due to an isolated human error.

FOUNDATIONS OF LAW

Yo

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

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

The Spanish Agency for Data Protection is competent to resolve this

process.

II

In relation to the arguments presented to the resolution proposal, the

THE CITY HALL insists again on the fact that there was no lack of diligence

for its part in the resolution of the security breach, but rather that this was due to the

albur that the public employees filed a claim with the AEPD instead of

inform, as indicated that it was his duty, to the person responsible for the treatment of the data breach.

security occurred. Thus, it considers that this negligent action of the employees

which caused a late action by the City Council.

However, the claimant did not act in his capacity as a public employee linked

by a statutory relationship to the City Council and, therefore, obliged to communicate the

incidence within the framework of its statutory duties, but acted as an interested party,

affected by the security breach, having all the legitimacy to

claim directly from the AEPD, as permitted by law.

The CITY COUNCIL is charged with the commission of an infraction for violation of the

Article 5.1.f) of the GDPR, article 32 GDPR and article 33 GDPR.

III

Article 5.1.f) RGPD 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").”

The aforementioned infringement of article 5.1.f) of the RGPD could lead to the commission of the

offenses typified in article 83.5 of the RGPD that under the heading "Conditions

rules for the imposition of administrative fines" provides:

“Infractions of the following provisions will be sanctioned, in accordance

with paragraph 2, with administrative fines of EUR 20,000,000 as

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

as a maximum of the overall annual total turnover of the financial year

above, opting for the highest 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 the regulations constitute infractions.

paragraphs 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as the

that are contrary to this organic law.

For the purposes of the statute of limitations, article 72 “Infringements considered

very serious” of the LOPDGDD indicates:

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

2016/679 are 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. (…)”

Given that it has been shown throughout the instruction of the procedure, that the

data of 126 public employees have been unduly exposed, due to the

publication of the Minutes of the Governing Board dated 10/21/2020 in the BOP, data

that should not be accessible to third parties by virtue of the provisions of article 70

of Law 7/1995 of April 2, regulating the Bases of Local Regime, in relation

with article 18 of Law 40/2015 of October 1, on the Legal Regime of the Sector

Public, the infringement of the aforementioned article 5.1.f) of the RGPD is accredited.

IV

Article 83 section 7 of the RGPD, provides the following:

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."

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

autonomous communities 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.

(…)

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. (…)"

v

Article 32 “Security of treatment” of the RGPD establishes:

"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 violation of article 32 of the RGPD could lead to the commission of the infractions 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 pursuant to 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 a level of security appropriate to the risk

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

(EU) 2016/679.

(…)

The fact that the personal data of public employees were published in the

BOP without having previously proceeded to its anonymization, indicates that the

City Council did not have the appropriate organizational and technical measures, so

that the infringement of the aforementioned article 32 of the RGPD is considered to have been committed. The

The City Council affirms that the security breach occurred as a result of an error

human. Well, appropriate organizational and technical security measures have

to guarantee a level of security appropriate to the risk considering, at all points,

all the risks present in the processing of personal data. So the mistake

human is a risk factor present in all treatments involving

people, which implies that it must be duly considered and implemented

all appropriate security measures to avoid them. It is necessary to have

adequate measures that prevent, due to human error, the occurrence of

situations such as the one substantiated in this proceeding.

SAW

Article 83 section 7 of the RGPD, provides the following:

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."

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

autonomous communities 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.

(…)

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. (…)"

Article 33 "Notification of a violation of the security of personal data to

the control authority" of the RGPD establishes:

7th

"1. In case of violation of the security of personal data, the person in charge of the

treatment will notify the competent control authority in accordance with the

article 55 without undue delay and, if possible, no later than 72 hours after

who was aware of it, unless it is unlikely that such violation

constitutes a risk to the rights and freedoms of individuals

physical. If the notification to the supervisory authority does not take place within the period of 72

hours, must be accompanied by an indication of the reasons for the delay.

2. The person in charge of the treatment will notify without undue delay the person in charge of the

treatment the violations of the security of the personal data of which it has

knowledge.

3. The notification referred to in section 1 must, at a minimum:

a) describe the nature of the data security breach

including, where possible, the categories and number

approximate number of stakeholders affected, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

4. If it is not possible to provide the information simultaneously, and to the extent that

is not, the information will be provided gradually without undue delay.

5. The data controller will document any breach of data security.

personal data, including the facts related to it, its effects and the

corrective measures taken. Said documentation will allow the authority of

control to verify compliance with the provisions of this article."

The violation of article 33 of the RGPD could lead to the commission of the infractions

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,

treating

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

Total annual global business of the previous financial year, opting for the one with the highest

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; (…)"

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/12

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

following:

(…)

r) Failure to comply with the duty to notify the data protection authority

data from a security breach of personal data in accordance

with the provisions of article 33 of Regulation (EU) 2016/679. (…)”

In the present case, it is clear that the notification of the security breach to the AEPD was

occurred after the period indicated in article 33 of the RGPD, without there being

any type of circumstances that support undue delay.

viii

Article 83 section 7 of the RGPD, provides the following:

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.”

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

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

(…)

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 results

authority will issue a resolution sanctioning them with a warning.

The resolution will also establish the measures to be adopted so that

stop the conduct or correct the effects of the infraction that had occurred.

task.

(…)

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. (…)"

IX

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 Agency for Data Protection, RESOLVES:

FIRST: SANCTION SAN JAVIER CITY COUNCIL, with NIF P3003500J,

for an infringement of Article 5.1.f) of the RGPD, with a WARNING.

SANCTION the CITY COUNCIL OF SAN JAVIER, with NIF P3003500J, for a

violation of Article 32 of the RGPD, with a WARNING.

SANCTION the CITY COUNCIL OF SAN JAVIER, with NIF P3003500J, for a

infringement of Article 33 of the RGPD, typified in Article 83.5 of the RGPD, with a

WARNING.

SECOND: NOTIFY this resolution to the SAN JAVIER CITY COUNCIL.

THIRD: 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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es