 File No.: PS/00158/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: On November 18, 2020, Ms. A.A.A. (hereinafter the part claimant) filed a claim with the Spanish Data Protection Agency, against the CITY COUNCIL OF ARNUERO, with NIF P3900600B, (hereinafter, the claimed).

The claimant states that the son of a neighbor of the municipality of Arnuero filed a complaint against her, providing along with that complaint, an email that she same sent to the City Council on ***DATE.1. It states that the City Council provided this person with a copy of his writing in which his data was recorded without having concealed them and that the necessary measures were not adopted to ensure compliance with data protection regulations. in said mail email you could see your name, surnames, ID, address, mobile phone and address of e-mail.

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 respondent, so that proceed to 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.

On February 22, 2021, a response letter was received from the respondent in the which shows that an official letter is sent to the company ***EMPRESA.1., with which

the City Council had contracted, on that date, advice on matters of

protection of personal data, and states that:

- Until January 25, no report is issued by the

***EMPRESA.1 and this only after various telephone procedures. The indicated report

receives entry number 2021-E-RC-XXX, also dated January 25, having been sent to

this City Council by email, along with another that was requested from the indicated

company, about the document filed by a third party before this City Council.

- Considering the terms of the report regarding the claim to be insufficient, the day

January 29, 2021, a new communication is sent by email to the

representation of ***EMPRESA.1, urging greater precision and scope on the

issues that had been consulted, given that it was considered that what was raised

from the AEPD, made it necessary before adopting any resolution.

- In relation to the additional report thus requested, until the date of issuance of the

present, no news. All of which is made known to the

Effects of being taken into account in the processing of actions with s./ref. AND/

10291/2020, indicating that they have been circumstances totally beyond the will

which have prevented a full response to what was required, especially

in relation to the sections through which it is required "the decision adopted to

purpose of this complaint” and the “report on the measures adopted to avoid

that similar incidents occur, dates of implementation and controls carried out

to verify its effectiveness”, given that it is estimated that all of this needs to receive

adequate technical-legal support.

THIRD: On April 8, 2021, in accordance with article 65 of the

LOPDGDD, the Director of the Spanish Data Protection Agency agreed

admit for processing the claim filed by the claimant against the respondent.

FOURTH: On November 26, 2021, the Director of the Spanish Agency for

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

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

typified in article 83.5 and 83.4 of the RGPD, respectively.

Once the initiation agreement was notified, the respondent filed a brief with allegations in

which, in summary, stated that it had proceeded to implement the measures

adequate corrective measures to avoid the repetition of similar events in the future and

requested the file of the sanctioning procedure.

FIFTH: On January 27, 2022, a resolution proposal was formulated,

proposing:

<< That by the Director of the Spanish Agency for Data Protection, the

CITY COUNCIL OF ARNUERO, with NIF P3900600B, for a violation of article

5.1. f) of the RGPD, in accordance with the provisions of article 83.5 of the RGPD, qualified

as very serious for prescription purposes in article 72.1 i) of the LOPDGDD and

infringement of article 32 of the RGPD, in accordance with the provisions of article 83.4 of the

cited RGPD, qualified as serious for prescription purposes in article 73

section f) of the LOPDGDD, a sanction of warning. >>

SIXTH: The respondent party has not submitted arguments to the Proposal for

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 stated that on November 18, 2020, the complaining party

filed a claim with the Spanish Agency for Data Protection, since

the party complained against provided a third party with a copy of his brief containing

your personal data without having hidden them.

SECOND: It is verified that it is an email in which you can

display name, surnames, ID, address, mobile phone and email address

email of the claimant, for which third parties had unauthorized access

to said data.

THIRD: The respondent states that he has proceeded to implement the measures

adequate corrective actions to avoid the repetition of similar events in the future. The

documentation provided is incorporated into the file.

FOUNDATIONS OF LAW

FIRST: In accordance with the powers that article 58.2 of the 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."

SECOND: 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 "Principles related to treatment" of the RGPD, section 1.f), when disclosing information and personal data to third parties.

THIRD: Regarding the security of personal data, article 32 of the RGPD "Security of treatment", establishes that:

"1. Taking into account the state of the art, the application costs, and the nature, scope, context and purposes of the treatment, as well as risks of

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. (The underlining is from the AEPD).

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.

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 liability of the claimed party is determined by the security breach

revealed by the claimant, since he is responsible for making decisions

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.

The lack of security measures is proven, in addition to the result of re-

disclosure of information, containing personal data, due to the fact that the City Council

in its response to this Agency, it undertakes to adopt a number of

These basic security measures, previously non-existent. For example “Set a

Policy for the use of the City Council information system.”

FOURTH: Article 83.5 of the RGPD provides the following:

"5. Violations of the following provisions 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)

basic principles for treatment, including conditions for con-

sentiment under articles 5, 6, 7 and 9;”

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what

following: Violations constitute the acts and conducts referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

For the purposes of the limitation period for infractions, article 72 of the LOPDGDD,

under the rubric of infractions considered very serious, it establishes the following: “1. In

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.”

The violation of article 32 RGPD is typified in article 83.4.a) of the

cited RGPD in the following terms:

"4. Violations of the following provisions 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.”

(…)

For the purposes of the limitation period for infractions, article 73 of the LOPDGDD,

under the heading "Infringements considered serious", it establishes the following:

“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 result

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

in the terms required by article 32.1 of Regulation (EU) 2016/679.

In the present case, the infringing circumstances provided for in article

83.5 and 83.4 of the GDPR.

FIFTH: Establishes Law 40/2015, of October 1, on the Legal Regime of the Sector

Public, in Chapter III on the "Principles of the power to sanction", in the

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.

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

all of 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;”

The imposition of this last measure is compatible with the sanction consisting of

administrative fine, as provided in art. 83.2 of the GDPR.

SEVENTH: Article 83.7 of the RGPD adds:

“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.”

The Spanish legal system has chosen not to penalize with the imposition of

administrative fine to public entities but with a warning, as

indicated in article 77.1. c) and 2. 4. 5. and 6. of the LOPDGDD:

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.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

sufficient evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on disciplinary or sanctioning regime that

result of application.

Likewise, when the infractions are attributable to authorities and managers, and

proves the existence of technical reports or recommendations for the treatment 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 notified of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

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.

6. When the competent authority is the Spanish Data Protection Agency,

this will publish on its website with due separation the resolutions referring 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 infraction.

When the competence corresponds to a regional authority for the protection of

data will be, in terms of the publicity of these resolutions, to what your

specific regulations."

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

ARNUERO, with NIF P3900600B, for a violation of article 5.1. f) of the RGPD and of the

article 32 of the RGPD, typified in articles 83.5 of the RGPD and 83.4 of the RGPD,

respectively.

SECOND: REQUEST the CITY COUNCIL OF ARNUERO, to implement the

necessary corrective measures to adapt their actions to the regulations of

protection of personal data, which prevent events from being repeated in the future

Similar.

THIRD: NOTIFY this resolution to the CITY COUNCIL OF ARNUERO.

FOURTH:

in accordance with the provisions of article 77.5 of the LOPDGDD.

COMMUNICATE this resolution to the Ombudsman,

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

938-150222

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es