 File No.: PS/00369/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: On January 27, 2021, D. A.A.A. (hereinafter, the claimant) filed a claim with the Spanish Agency for Data Protection, against the CITY COUNCIL OF ALICANTE/ALACANT, with NIF P0301400H, (hereinafter, the reclaimed). The grounds on which the claim is based are a possible violation of the data protection legislation, produced after the notification of a resolution that contained someone else's data. Along with the claim, provide a copy of the resolution addressed to the claimant, but containing the data of another citizen.

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.

There is no record in this Agency of a reply to the transfer of the claim.

THIRD: On May 12, 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: 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 May 17, 2021, information was requested from the respondent and the response

received the following follows:

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

the adverse effects and measures adopted for their final resolution:

 The claimant filed an application for the refund of fees in

dated September 19, 2019, which was dismissed on September 19,

November 2019.

 Article 57 of Law 39/2025 of October 1 on procedure

common administrative allows the accumulation of applications in a single

file (The administrative body that initiates or processes a procedure, anyone who

has been the form of its initiation, it may have, ex officio or at the request of a party, its

accrual to others with whom he or she has a substantial identity or intimate connection, provided that it is

the same body who must process and resolve the procedure) so they proceeded to

the accumulation in a single file of various identical applications and the

joint dismissal of all of them.

The resolution is joint, but the notification to the interested parties is only included

the part that affects them.

The respondent has provided a copy of the resolution of the procedure

dismissal dated 11/14/2019 where the personal data of the

claimant along with 8 other people.

 The respondent states that (...)

A copy of the notification has been provided (...). Both notices are from

11/19/2019.

The respondent states that there has been no violation in the

data protection regulations regarding the claimant.

 On December 20, 2019, the claimant filed an appeal in the

which, among other aspects, revealed the error in its notification and

part of the respondent was sent a new notification on January 29, 2020

with the correct data.

This appeal was estimated by the Economic-Administrative Tribunal

municipal on February 8, 2021 proceeding to the return of the

claimed fees.

FIFTH: On July 23, 2021, the Director of the Spanish Agency for

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

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), 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 respectively of the RGPD.

SIXTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written

allegations in which, in summary, it stated that the data of

a third party to the claimant due to human confusion, caused by the large number

of resolutions that the City Council must notify.

SEVENTH: On October 22, 2021, a resolution proposal was formulated, in

the following terms:

<< That the Director of the Spanish Agency for Data Protection directs a

warning to the CITY COUNCIL OF ALICANTE/ALACANT, with NIF P0301400H,

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 the article

72.1 i) of the LOPDGDD and for violation of article 32 of the RGPD, in accordance with the

provided in article 83.4 of the aforementioned RGPD, classified as serious for the purposes of

prescription in article 73 section f) of the LOPDGDD.>>

EIGHTH: On November 10, 2021, the entity claimed filed a written

of allegations to the Resolution Proposal, in which, in summary, it stated that

the data of the claimant were not communicated to anyone else, that the erroneous

communication of the data was due to an error, that said error was of a

exceptional and was produced by a human confusion, confusion that had not been

produced up to that date after the processing of thousands of notifications and that no

reiterated since then by having the City Council with techniques and procedures that

guarantee an adequate level of security, states that they are going to improve the

security measures to avoid the repetition of similar events in the future and

requests the filing of the proceedings without imposing any sanction.

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: On 11/11/19 the claimant is notified of a resolution that

contained someone else's data.

SECOND: From the documentation presented by the claimed party, due to an error

the claimant was notified of a third party's data, but the claimant's data was not

have notified third parties.

FOUNDATIONS OF LAW

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

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

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

and to solve this procedure.

SECOND: Regarding the allegations presented to the Resolution Proposal, it is

should point out that security measures must be adopted in attention to all and

each of the risks present in the processing of personal data,

including among them, the human factor.

This risk must be taken into account by the data controller who, in

function of this, must establish the necessary technical and organizational measures that

prevents the data controller from losing control of the data and,

therefore, by the owners of the data that provided them.

In this sense, it has been found that the security measures available

implemented by the claimed entity in relation to the data that it submitted to treatment

as the person in charge, were not adequate to enable the exhibition to third parties

of personal data with the consequent lack of diligence by the

responsible.

Consequently, the allegations must be dismissed, meaning that the

arguments presented do not distort the essential content of the infraction that

declared to have been committed, nor do they imply sufficient cause for justification or exculpation.

THIRD: The defendant is accused of committing an infraction for

Violation of article 5.1.f) of the RGPD and article 32 of the RGPD.

Article 5.1.f) of the RGPD, Principles related to treatment, states the following:

"1. The personal data will be:

(…) f) processed in such a way as to guarantee 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 ("integrity and confidentiality").

Article 5 of the LOPDGDD, Duty of confidentiality, states the following:

"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 to the

duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even

when the relationship of the obligor with the person in charge or in charge of the

treatment".

The documentation in the file shows that the defendant,

violated article 5.1.f of the RGPD, principles related to treatment, in relation to the

Article 5 of the LOPGDD, duty of confidentiality, when sending a resolution to the

claimant, revealing information and personal data of a third party.

This duty of confidentiality must be understood to have the purpose of preventing

leaks of the data are carried out without the consent of the owners of these.

Therefore, this duty of confidentiality is an obligation that falls not only on the

responsible 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.

Furthermore, article 40.5 of the LPACAP establishes that "The

Public Administrations may adopt the measures they deem necessary

for the protection of personal data contained in resolutions and acts

administrative, when these have as addressees more than one interested party"; given

that there had been an accumulation of several proceedings under article

57 of the same legal text, the precautions established

normatively.

FOURTH: 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 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 such 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 violation of the measures

technical and organizational by enabling the exhibition to third parties of documentation where

contain personal data with the consequent lack of diligence by the

responsible.

Security measures must be adopted in attention to each and every one of the

risks present in the processing of personal data, including, among

the same the human factor.

FIFTH: The GDPR defines breaches of personal data security as

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

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

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

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

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

security when notifying the claimant of information and personal data in a resolution

from a third party.

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.
In this case, as evidenced by the facts and in the case file
E/05586/2021, the AEPD transferred to the respondent, the claim submitted for
analysis, requesting the provision of information related to the incident. In the

documentation provided, the respondent acknowledges that he made a mistake and notified a resolution containing personal data of a third party.

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.

In accordance with the foregoing, the respondent is responsible for the violation of the article 32 of the RGPD, infringement typified in article 83.4.a) of the RGPD.

SIXTH: 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) the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9;"

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what following: "The acts and behaviors 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:

(…)

Yo)

The violation of the duty of confidentiality established in article 5

of this organic law.

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, transcribed above.

SEVENTH: 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.

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

all of the following corrective powers indicated below:

b) send a warning to any person responsible or in charge of the treatment when the treatment operations have violated the provisions of this Regulation;

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.

NINTH: 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 fine entities public 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

of interested, in his case."

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."

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: DIRECT TO THE CITY COUNCIL OF ALICANTE/ALACANT, with NIF

P0301400H, for a violation of article 5.1.f) of the RGPD and article 32 of the RGPD,

typified in article 83.5 of the RGPD, a warning.

SECOND: NOTIFY this resolution to the CITY COUNCIL OF

ALICANTE/ALACANT.

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

938-26102021

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es