 Procedure No.: PS/00376/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following:

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) dated June 15, 2020

filed a claim with the Spanish Data Protection Agency.

The claim is directed against ASESORÍA MUNIZ SOLAN, S.L. with NIF B21451364

(hereinafter, the claimed).

The grounds on which the claim is based are that, as Vice President of the

Intercommunity of owners to which it belongs, states that when requesting a copy of

an issued certificate of debt claim of a debtor co-owner, but in

instead of sending him the correct one, they sent him a copy of a certificate belonging to a

third, violating the duty of confidentiality.

A copy of the debt certificate issued in the name of a third party, dated 15

January 2020.

SECOND: The present claim was transferred to the respondent on June 25, 2020 and

was reiterated on July 13, 2020, requiring that within a month

forward to this Agency, information on the causes that have motivated the incidence

which gave rise to the claim, report on the measures taken to prevent

similar incidents occur, dates of implementation and controls carried out

to verify its effectiveness, but the entity complained against has not answered within the period

indicated.

THIRD: On October 16, 2020, in accordance with article 65 of the

LOPDGDD, the Director of the Spanish Data Protection Agency agreed to admit

processing the claim filed by the claimant against the claimed.

FOURTH: On December 15, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimed party, 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 alleged violations of articles 5.1.f) and 32 of the RGPD,

typified in articles 83.5 a) and 83.4 a) of the RGPD.

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

allegations in which, in summary, he requests: "the annulment of the file for not going

directed to the correct person and the annulment of the file for being defenseless this

company that has not been able to know previously what was cooking in this matter ”.

SIXTH: On December 29, 2020, the instructor of the procedure agreed to the

opening of a period of practice tests, considering incorporated the

previous investigative actions, E/05269/2020, as well as the documents

provided by the claimant.

SEVENTH: On February 3, 2021, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

sanction ASESORÍA MUNIZ SOLÁN, S.L., with NIF B21451364, for infractions

of articles 5.1 f) and 32 of the RGPD, typified in articles 83.5 a) and 83.4 a) of the

GDPR respectively.

□

for the infringement of article 32 of the RGPD, typified in article 83.4 a) of the

RGPD, the corresponding sanction would be a warning, requiring the

demanded that it proceed to adopt the necessary measures to stop the

conduct that is the subject of this complaint, which has caused the security breach

denounced, the effects of the infraction committed and its adequacy to the

requirements contemplated in article 32 of the RGPD, as well as the contribution

of means accrediting compliance with what is required.

for the infringement of article 5.1 f) of the RGPD, typified in article 83.5 a) of the

RGPD the sanction that would correspond would be a fine for an amount of 2,000

euros (two thousand euros) without prejudice to what results from the instruction.

EIGHTH: Once the proposed resolution was notified, the party complained against submitted a written

of allegations ratifying those made to the Home Agreement, requesting the

nullity of the file.

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

1.- The party claimed through the Secretary-Administrator D. B.B.B., sent to the

claimed, as Vice President of the Intercommunity of owners, a copy of a

certificate issued on January 15, 2020 of debt claim of a

debtor co-owner, but instead of sending him the correct one, they sent him a copy of a

certificate belonging to a third party, violating the duty of confidentiality.

2.- The claimant provides a copy of the debt certificate issued in the name of a

third, dated January 15, 2020.

FOUNDATIONS OF LAW

Yo

The Director of the Spanish Agency is competent to resolve this procedure.

Data Protection, in accordance with the provisions of art. 58.2 of the GDPR and

in the

art. 47 and 48.1 of LOPDGDD.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

II

The joint assessment of the documentary evidence in the procedure brings to

knowledge of the AEPD, a vision of the denounced action that has been re-

reflected in the facts declared proven above reported.

However, in response to the allegations presented by the respondent entity,

should point out the following:

Regarding the statement made by the respondent entity when it indicates that "the annulment of the

file for not being addressed to the correct person". On this particular, we must

point out that in this sanctioning procedure there is a certificate issued on

January 15, 2020 by the claim through the Secretary-Administrator, addressed to

claimant as Vice President of the Intercommunity of owners on a

debt claim of a debtor co-owner, but instead of sending the

correct, they sent him a copy of a certificate belonging to a third party, violating the

duty of confidentiality. Therefore, the responsibility of the

claimed in the remission of the debt certification.

In relation to "the annulment of the file for being defenseless this company that does not

has been able to know previously what was cooking in this matter ". It is important to highlight

that electronic notification was made, as established in article 14.2.a) of

Law 39/2015 LPACAP, and the Notification Service Support service

Electronic and Authorized Electronic Address certifies that the date of implementation

disposition was 06/25/2020 16:05:43 and the automatic rejection date was 07/06/2020

00:00:00 The automatic rejection occurs, in general, after having elapsed

ten calendar days from its availability for access according to paragraph 2,

Article 43 of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations. Subsequently, it was notified by the service of

post office on 07/16/2020, being returned on the 28th of the same month and year.

Article 43 of Law 39/2015, in section 3, establishes: “it shall be understood that

the obligation referred to in article 40.4 with the provision of the

notification in the electronic headquarters of the Administration or Acting Body or in the

unique authorized electronic address”.

Therefore, it is considered that the existence of “a

radical defect of nullity of the present procedure”, as defended by the entity

claimed.

In this way, it is fully accredited that there has been no defenselessness.

The RGPD establishes in article 5 the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

III

The article notes 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 or unlawful processing and

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

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

In turn, the security of personal data is regulated in article 32

of the GDPR.

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.

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 controller or the

manager and has access to personal data can only process said data

following the 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 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,

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.

(…)"

For its part, the LOPDGDD in its article 71, Violations, states 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.

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

considered serious”:

“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:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance with

required by article 32.1 of Regulation (EU) 2016/679”.

IV

The GDPR defines personal data security breaches 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 of

that the claimed party has violated article 32 of the RGPD, when there was a breach of

security in their systems by sending a copy of the amount claim of a

third party, to the claimant, to whom he informs of the debt contracted by the third party.

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 the treatment entails, taking into account the state of the art, the costs of application, 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 measures technical and organizational information must be carried out taking into account: pseudonymization and encryption, the ability to ensure the confidentiality, integrity, availability and resiliency, the ability to restore availability and access to data after a incident, verification process (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 provisions of 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 ensure an adequate level of security, including the

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.

v

According to the available evidence and the

documentation provided shows that the claimant requested a copy of the certificate

issued by the secretary-administrator of your intercommunity of owners of

debt claim from a debtor co-owner, but instead of sending the correct one,

sent a copy of a certificate belonging to a third party, violating the duty of

confidentiality, which constitutes, on the part of the claimed, two infractions, one

against the provisions of article 32 of the RGPD and another against the provisions of article

5.1 f) of the RGPD, which governs the principles of data integrity and confidentiality

personal data, as well as the proactive responsibility of the data controller

demonstrate compliance.

SAW

Article 58.2 of the RGPD provides the following: "Each supervisory authority

shall have all of the following corrective powers listed below:

b) sanction any person responsible or in charge of the treatment with

warning when the processing 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 certain way and within a specified period;

i) impose an administrative fine under article 83, in addition to or in

instead of the measures mentioned in this paragraph, depending on the circumstances

of each particular case;

Article 72.1.a) of the LOPDGDD states that “according to what is established

Article 83.5 of Regulation (EU) 2016/679 are considered very serious and

Infractions that suppose a substantial violation will prescribe after three years.

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.

This infraction can be sanctioned with a fine of €20,000,000 maximum.

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

of greater amount, in accordance with article 83.5 of the RGPD.

In accordance with the provisions of the RGPD in its article 83.2, when deciding the imposition

of an administrative fine and its amount in each individual case shall be taken into account

the aggravating and mitigating factors that are listed in the aforementioned article, as well

as well as any other that may be applicable to the circumstances of the case.

Consequently, the following have been taken into account as aggravating factors:

 In the present case we are dealing with gross negligence (article 83.2 b).

 Basic personal identifiers (name, surname) are affected.

two, domicile), according to article 83.2 g).

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: IMPOSE ASESORÍA MUNIZ SOLÁN, S.L., with NIF B21451364, for the

following offenses:

for the infringement of article 32 of the RGPD, typified in article 83.4 a) of the

RGPD the sanction would be a warning requiring the claimed party

to proceed, within a period of one month, to adopt the necessary measures to

cessation of the conduct that is the subject of this claim, which has caused the breach

of security denounced, so that the effects of the infraction are corrected

committed and its adaptation to the requirements contemplated in article 32 of the

RGPD, as well as the provision of accrediting means of compliance with the

required.

for the infringement of article 5.1 f) of the RGPD, typified in article 83.5 a) of the

RGPD the sanction would be a fine for an amount of 2,000 euros (two thousand

euros).

SECOND: NOTIFY this resolution to ASESORÍA MUNIZ SOLÁN, S.L..

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure
Common Public Administrations (hereinafter LPACAP), within the payment term
voluntary established in art. 68 of the General Collection Regulations, approved
by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,
of December 17, through its entry, indicating the NIF of the sanctioned and the number
of procedure that appears in the heading of this document, in the account
restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency
Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case
Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is
between the 1st and 15th of each month, both inclusive, the term to make the payment
voluntary will be until the 20th day of the following month or immediately after, and if
between the 16th and last day of each month, both inclusive, the payment term
It will be until the 5th of the second following month or immediately after.

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

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es