Procedure No.: PS/00483/2020

 RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Mr. A.A.A., representative of Ms. B.B.B. (hereinafter the claimant), with

date 06/30/2020 filed a claim with the Spanish Agency for the Protection of

Data. The claim is directed against ASESORÍA ALPI-CLÚA, S.L. with NIF

B63056162 (hereinafter, the claimed one). The grounds on which the claim is based are,

in summary, that the claimant requested the necessary documentation for certain procedures

before the Treasury to said entity, and the latter, by email, sent him a

document in which personal data of another client appears. Provide the email and a

receipt of presentation of documentation to the Treasury by the Advisory, with

indication of data from another client.

SECOND: Upon receipt of the claim, the Subdirectorate General for Inspection

tion of Data proceeded to carry out the following actions:

On 08/05/2020, reiterated on 08/31/2020, the claim was transferred to the defendant

submitted for analysis and communication to the claimant of the decision adopted

regard. Likewise, it was required that within a month he send to the

Agency certain information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent incidents from occurring.

similar quotes.

- Any other that you consider relevant.

There is no evidence that the respondent has given any response to the request of the

AEPD.

THIRD: On 12/17/2020, in accordance with article 65 of the LOPDGDD, the Di-

Rector of the Spanish Agency for Data Protection agreed to admit for processing the re-

claim filed by the claimant against the respondent.

FOURTH: On 01/25/2021, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged in-

fractions of articles 5.1.f) and 32.1 of the RGPD, sanctioned in accordance with the provisions

to in articles 83.5.a) and 83.4.a) of the aforementioned RGPD.

FIFTH: Once the initiation agreement has been notified, the person claimed at the time of this resolution

tion has not submitted a brief of allegations, so what is indicated is applicable

in article 64 of Law 39/2015, of October 1, on Administrative Procedure

Common of the Public Administrations, which in its section f) establishes that in case

of not making allegations within the stipulated period on the content of the initial agreement

ciation, it may be considered a resolution proposal when it contains a pro-

precise statement about the imputed responsibility, so we proceed to

dictate Resolution.

SIXTH: Of the actions carried out in this proceeding, they have been

accredited the following:

PROVEN FACTS

FIRST: Mr. A.A.A., representative of Ms. B.B.B. (hereinafter the claimant), with

date 06/30/2020 filed a claim with the Spanish Agency for the Protection of

Data stating that you requested the requested documentation necessary to carry out

carried out procedures before the AEAT and, by email, sent him a document in

in which personal data of another client appears.

SECOND: A copy of the representative's DNI, number ***DNI.1, has been provided.

THIRD: A copy of the sent email and a pre-payment receipt are provided.

presentation of the extension of the term for completing the procedures before the AEAT, in which

contains personal data corresponding to a third party.

FOUNDATIONS OF LAW

Yo

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

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

rector of the Spanish Agency for Data Protection is competent to initiate and

to solve this procedure.

II

Law 39/2015, of October 1, on the Common Administrative Procedure of

the Public Administrations, in its article 64 “Initiation agreement in the procedures

sanctions of a punitive nature”, provides:

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the regulatory norms

of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible qualification

tion and the sanctions that may correspond, without prejudice to what is

of instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and rule that attributes it.

buy such competence, indicating the possibility that the alleged perpetrator

can voluntarily acknowledge its responsibility, with the effects foreseen

in article 85.

e) Provisional measures that have been agreed by the competent body.

competent to initiate the sanctioning procedure, without prejudice to those

may adopt during the same in accordance with article 56.

f) Indication of the right to make allegations and to be heard in the proceeding.

procedure and the deadlines for its exercise, as well as an indication that, in the event

not to carry out

allegations within the stipulated period on the content of the

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the im-

bitch.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out at a later stage.

through the preparation of a List of Charges, which must be notified to the

interested".

In application of the previous precept and taking into account that no

side arguments to the initial agreement, it is appropriate to resolve the initiated procedure.

III

The claimed facts that have given rise to this proceeding are

They carry out the disclosure of personal data when an email is sent to the claimant

electronically with a document belonging to a third party in which they were contained with

breach of the technical and organizational measures violating the confidentiality

ness of the data.

Article 58 of the RGPD, Powers, states:

"two. Each control authority will have all the following powers:

rectives listed below:

(…)

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

when the treatment operations have violated the provisions of the

this Regulation;

(…)"

Article 5, Principles relating to processing, of the GDPR states that:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing

to and against accidental loss, destruction or damage, through the application of

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

(…)

Also article 5, Duty of confidentiality, of the new Organic Law

3/2018, of December 5, on the Protection of Personal Data and guarantee of the rights

digital rights (hereinafter LOPDGDD), states that:

"1. Those responsible and in charge of data processing as well as all

people who intervene in any phase of this will be subject to the duty of confidentiality

referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary

of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain

even when the relationship of the obligor with the person in charge or person in charge had ended

of the treatment".

IV

The documentation in the file offers evidence that the claimed,

violated article 5 of the RGPD, principles related to treatment, in relation to the ar-

Article 5 of the LOPGDD, duty of confidentiality, when documents are sent by e-mail.

containing personal data of a third party.

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

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

felt by their owners.

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

only to the person in charge and in charge of the treatment but to everyone who intervenes in

any phase of the treatment and complementary to the duty of professional secrecy.

v

Article 83.5 a) of the RGPD, considers that the infringement of “the basic principles

costs for treatment, including the conditions for consent under the

articles 5, 6, 7 and 9” is punishable, in accordance with section 5 of the aforementioned article.

Article 83 of the aforementioned RGPD, "with administrative fines of €20,000,000 maximum

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

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

of greater amount”.

The LOPDGDD in its article 72 indicates: “Infringements considered very serious:

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

2016/679 are considered very serious and the infractions that

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

ticular, the following:

a) The processing of personal data violating the principles and guarantees established

established in article 5 of Regulation (EU) 2016/679.

(…)

SAW

Second, article 32 of the RGPD “Security of treatment”, establishes

ce 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 pro-

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

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

appropriate channels to guarantee a level of security appropriate to the risk, which in its

case include, among others:

a) pseudonymization and encryption of personal data;

b) the ability to guarantee the confidentiality, integrity, availability and re-

permanent silence of treatment systems and services;

c) the ability to restore availability and access to personal data

promptly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the treatment

I lie.

2. When evaluating the adequacy of the security level, particular consideration shall be given to

taking into account the risks presented by the processing of data, in particular as a consequence

accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or unauthorized access

torized to such data.

3. 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

feel article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee

warrant that any person acting under the authority of the person in charge or the person in charge

do and have access to personal data can only process said data following instructions

instructions of the person in charge, unless it is obliged to do so by virtue of the Law of the

Union or of the Member States.

7th

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

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

"4. Violations of the following provisions will be sanctioned, in accordance

with paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or, alternatively,

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

overall annual total turnover of the previous financial year, opting for the

greater amount:

a) the obligations of the person in charge and the person in charge pursuant to articles 8,

11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "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

following:

(…)

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

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

to what is required by article 32.1 of Regulation (EU) 2016/679".

(…)"

viii

The GDPR defines personal data security breaches as "all

all those security violations that cause the destruction, loss or alteration

accidental or illicit ration of personal data transmitted, conserved or processed in

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

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

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

security in your system allowing access to personal data of a third party, by

be forwarded mail allowing access to the document that contained them with break-

treatment of the established measures.

It should be noted that the RGPD in the aforementioned provision does not establish a list of

the security measures that are applicable according to the data that is

object of treatment, but it establishes that the person in charge and the person in charge of the treatment

will apply technical and organizational measures that are appropriate to the risk that

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

cation, the nature, scope, context and purposes of the treatment, the risks of

probability and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate.

to the detected risk, pointing out that the determination of the technical and

Organizational activities must be carried out taking into account: pseudonymization and encryption,

capacity to guarantee confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (not audit), evaluation and assessment of the effectiveness of the measures you give.

In any case, when evaluating the adequacy of the security level, parti- taking into account the risks presented by the processing of data, as a consequence accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the communication or unauthorized access authorized to said data and that could cause physical, material and them or immaterial.

In this same sense, recital 83 of the RGPD states that:

"(83) In order to maintain security and prevent the processing from violating the established in this Regulation, the person in charge or the person in charge must evaluate the risks inherent to the treatment and apply measures to mitigate them, such as encryption. These measures must guarantee an adequate level of security, including confidentiality. taking into account the state of the art and the cost of its application with respect to regarding the risks and the nature of the personal data to be protected. To the assess the risk in relation to data security, should be taken into account the risks arising from the processing of personal data, such as the destruction accidental or unlawful loss, loss or alteration of transmitted personal data, conservation stored or otherwise processed, or unauthorized communication or access to such data, susceptible in particular to cause physical, material or

immaterial".

In the present case, as evidenced by the facts and within the framework of the

investigation tooth E/06014/2020 the AEPD transferred the claim to the defendant

submitted for analysis requesting the provision of information related to the

incident claimed, without any response having been received in this body.

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

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

tions aimed at effectively implementing the technical and organizational measures

appropriate to guarantee a level of security appropriate to the risk to ensure the

confidentiality of the data, restoring its availability and preventing access to the

in the event of a physical or technical incident. However, from the documentation provided

It follows that the entity has not only failed to comply with this obligation, but also

Furthermore, the adoption of measures in this regard is unknown, despite having transferred

do of the filed claim.

In accordance with the foregoing, it is estimated that the respondent would be presumed

fully responsible for the infringement of the RGPD: the violation of article 32, infringement

tion typified in article 83.4.a).

IX

In order to establish the administrative fine to be imposed, they must observe

The provisions contained in articles 83.1 and 83.2 of the RGPD, which indicate:

"1. Each control authority will guarantee that the imposition of the fines

in accordance with this article for infringements of these Regulations.

indicated in sections 4, 5 and 6 are in each individual case effective, proportionate

tioned and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances

of each individual case, in addition to or as a substitute for the measures contemplated

in article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the

nature, scope or purpose of the processing operation in question

as well as the number of interested parties affected and the level of damages and losses.

who have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the data controller or data processor.

taking into account the technical or organizational measures that have been applied

under articles 25 and 32;

e) any previous infringement committed by the person in charge or the person in charge of the treatment-

I lie;

f) the degree of cooperation with the supervisory authority in order to remedy

gave the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in

particular if the person in charge or the person in charge notified the infringement and, in such case,

what extent;

i) when the measures indicated in article 58, paragraph 2, have been ordered

previously against the person in charge or the person in charge in question in re-

relationship with the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms

certificates approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement.

In relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in its article

Article 76, "Sanctions and corrective measures", establishes that:

"two. In accordance with the provisions of article 83.2.k) of the Regulation (EU)

2016/679 may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatments

of personal data.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission of the offence.

e) The existence of a merger by absorption process after the commission

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when not mandatory, a data protection delegate.

h) The submission by the person in charge or person in charge, voluntarily

to alternative conflict resolution mechanisms, in those su-

positions in which there are controversies between them and any interested party."

cough.

- In accordance with the precepts transcribed, in order to set the amount of the

sanction of a fine to be imposed in the present case for the infraction typified in article

83.5.a) of the RGPD for which the claimant is responsible, in an initial assessment

Initially, the following factors are considered concurrent:

The merely local scope of the treatment carried out by the claimant entity

mada.

Only one person has been affected by the offending conduct.

The damage caused to the claimant, having to go to this claiming instance-

do the aforementioned facts.

The respondent entity does not record that it has adopted measures to prevent the

produce similar incidents; Nor has it responded to the information request.

of the Agency which affects the lack of cooperation with the authority

control capacity in order to remedy the infringement and mitigate the possible

adverse effects of it.

There is no evidence that the entity had acted maliciously, although

the performance reveals a serious lack of diligence.

The link between the offender and the processing of personal data

personal character.

The claimed entity is a small business.

Therefore, in accordance with the established graduation criteria, both

adverse and favorable, a penalty of 2,000 euros is imposed for violation of the

article 5.1.f) of the RGPD, to which the claimed party must respond.

- Secondly, for the purpose of setting the amount of the penalty of a fine to tax

ner in the present case for the infringement typified in article 83.4.a) of the RGPD of the

that the defendant is responsible, in an initial assessment, they are estimated concurrent

the following factors:

The merely local scope of the treatment carried out by the claimant entity

mada.

Only one person has been affected by the offending conduct.

The damage caused to the claimant, having to go to this claiming instance-

do the aforementioned facts.

The respondent entity does not record that it has adopted measures to prevent the

produce similar incidents; Nor has it responded to the information request.

of the Agency which affects the lack of cooperation with the authority

control capacity in order to remedy the infringement and mitigate the possible

adverse effects of it.

There is no evidence that the entity had acted maliciously, although

the performance reveals a serious lack of diligence.

The link between the offender and the processing of personal data

personal character.

The claimed entity is a small business.

Therefore, in accordance with the established graduation criteria, both

adverse and favorable, a penalty of 1,000 euros is imposed for violation of the

article 32.1 of the RGPD, of which the claimed party must respond.

In accordance with the applicable legislation and assessed the graduation criteria

of the sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE ASESORÍA ALPI-CLÚA, S.L., with NIF B63056162, for an in-

fraction of article 5.1.f) of the RGPD, typified in Article 83.5.a) of the RGPD, a

fine of €2,000 euros (two thousand euros).

SECOND: IMPOSE ASESORÍA ALPI-CLÚA, S.L., with NIF B63056162, for a

infringement of article 32.1 of the RGPD, typified in Article 83.4.a) of the RGPD, a

fine of €1,000 euros (one thousand euros).

THIRD: NOTIFY this resolution to ASESORÍA ALPI-CLÚA, S.L., with

NIF B63056162.

FOURTH: 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, of the Administrative Procedure Co-

of the Public Administrations (hereinafter LPACAP), within the term of payment

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 in the name of the Spanish Agency

Department of Data Protection at the banking entity CAIXABANK, S.A.. In case of

Otherwise, it will be collected during the executive period.

Received the notification and once executed, if the date of execution is

is between the 1st and 15th of each month, both inclusive, the term to carry out the voluntary payment will be until the 20th day of the following month or immediately after, and if is between the 16th and last day of each month, both inclusive, the term of the payment will be until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, the 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 LPA-CAP, the interested parties may optionally file an appeal for reconsideration before the Director of the Spanish Agency for Data Protection within a period of one month counting from the day following the notification of this resolution or directly contentious-administrative case before the Contentious-administrative Chamber of the Au-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 Jurisdiction Contentious-administrative diction, within a period of two months from the day following 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 LPA-CAP, the firm resolution may be provisionally suspended 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 city

tada Law 39/2015, of October 1. You must also transfer to the Agency the documentation

certifying the effective filing of the contentious-administrative appeal. Yes

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

nistrative within two months from the day following the notification of the pre-

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