 File No.: EXP202206966

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On September 21, 2022, the Director of the Spanish Agency

of Data Protection agreed to initiate a sanctioning procedure against LISMARTSA, S.L.

(hereinafter the claimed party). Once the initiation agreement has been notified and after analyzing the

allegations presented, on January 26, 2023, the proposal for

resolution which is transcribed below:

<<

File No.: PS/00473/2022

PROPOSED RESOLUTION OF SANCTION PROCEDURE

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

to the following:

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the claiming party) dated May 11,

2022 filed a claim with the Spanish Data Protection Agency. The

claim is directed against LISMARTSA, S.L. with NIF B78112679 (hereinafter, the

claimed party). The reasons on which the claim is based are the following:

The complaining party has received several emails, the last one dated

August 26, 2021, sent to a plurality of recipients without having used the

blind carbon copy functionality, leaving your email addresses visible

personal. A copy of the messages sent is provided.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, Protection of Personal Data and guarantee of digital rights (in

forward LOPDGDD), said claim was transferred to the claimed party, for

to proceed to its analysis and send to this Agency, within a period of one month, the

Next information:

1. The decision adopted regarding this claim.

2. In the event of exercising the rights regulated in articles 15 to 22 of the

GDPR, accreditation of the response provided to the claimant.

3. Report on the causes that have motivated the incidence that has originated the

claim.

4. Report on the measures taken to prevent incidents from occurring

similar, dates of implementation and controls carried out to verify their effectiveness.

5. Any other that you consider relevant.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was collected on June 27, 2022, as

It appears in the acknowledgment of receipt that is in the file.

THIRD: On July 27, 2022, this Agency received a letter of

response of the claimed party in which, in summary, it indicated:

- That the reason why you did not put the emails with a blind carbon copy is for

try to get a response from one of the recipients to whom the message was sent

mail, since the claimant was on leave due to temporary disability and

it was necessary to carry out the operation of the company in his absence.

- That the reason for which you have used personal email addresses

of the claimant was because her corporate email account had been deleted.

- That you have contracted the services of Conversia in order to comply with the regulations

in terms of data protection.

FOURTH: On August 11, 2022, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

FIFTH: On September 21, 2022, the Director of the Spanish Agency

of Data Protection agreed to initiate disciplinary proceedings against the claimed party,

pursuant to the provisions of articles 63 and 64 of the LPACAP, for the alleged

violation of article 5.1.f) of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter GDPR), typified in article 83.5.a) of the GDPR, and

for the alleged infringement of article 32 of the GDPR, typified in article 83.4.a) of the

GDPR.

The aforementioned initiation agreement was notified to the claimed party, in accordance with the rules

established in the LPACAP, on September 21, 2022.

SIXTH: With the registration date of October 4, 2022, the claimed party

requested an extension of the term to present allegations.

On May 6, 2022, the respondent was granted a new term to

submit claims.

SEVENTH: The claimed party submitted a pleadings brief on October 19,

2022, in which, in summary, he stated:

1.- Acknowledgment of their responsibility, "requesting the reduction of the sanction of the

20% provided for in the applicable regulations."

2.- Concurrence of a series of mitigating factors.

Regarding those established in article 83 of the GDPR, it is understood that the

following:

- That of section a), since "At no time has there been an intention to harm

none of the people involved, having been a communication with scope

limited with a small, determined and known number of recipients.

Additionally, the level of damages and losses is estimated as low, also having

take into account that measures will be applied to mitigate them (request to delete the

mail).

To this end, it indicates that it attaches as document No. 1 "mails between the claimant and the

recipients of emails sent by LISMARTSA"

- That of section b), since "At no time has there been intentionality in

harm the claimant. If only Lismartsa could carry on

after being the claimant who held the reins of the company during a

decade."

- That of section c), because "I cannot request the recipients of the emails to

delete the emails that are the subject of this procedure, because I have not informed of

said email addresses, and the recipients communicated with LISMARTSA

(with Lucía) through those addresses without using bcc."

For this purpose, it indicates that it attaches "mails sent and received to Lismartsa, with the

different emails that the claimant used at work with the computer of the

company: ***EMAIL.1; ***EMAIL.2; ***EMAIL.3; ***EMAIL.4; ***EMAIL.5.

He adds that he has hired a consulting firm specializing in regulatory compliance

as well as four formations in this regard.

It also indicates that "Currently we use the Bcc tool but the

recipient thinks that I have not informed all concerned and without asking

authorization forwards the mail to whomever it deems appropriate." Attach emails

electronics for that purpose.

- That of section e), since "As of the date of this writing, this entity has not had

no sanctions regarding the protection of personal data."

- That of section f), since "This party has been fully cooperative

with this control authority, and assumes the total commitment that it continues to be so

throughout the procedure. Among the contracted services, there is also the

advice on procedures before the control authority, so we

They will accompany all the measures that this authority deems necessary to apply."

- That of section g), since "Only the email data has been affected.

electronic (…)".

Regarding those established in article 76.2 of the LOPDGDD, he understands that

the following concur:

- That of section a), since "This is a totally punctual infraction and

exceptional, motivated by the need to maintain the operation of the company,

which included the management of payroll, having access to the accounting, return of

access keys to the headquarters, telephone devices that are not in the headquarters and are being

paying, managing rentals of company properties…”

- That of section b), since "The activity of the company is cleaning, so it does not

Its main activity is the processing of personal data for the development of

its economic activity.

- That of section c), because "No benefit has been obtained with the infringement,

quite the contrary, it was intended that the company would not go bankrupt due to the impossibility of

manage it (…).”

- That of section h), since "No right of any person has been affected."

minor or vulnerable group.”

3.- That the penalty of warning would be more proportional to the specific case,

“taking into account the measures adopted and the concurrent mitigating factors, as well as

the delicate economic situation in which we find ourselves.”

O: Attached as an annex is a list of documents in the

OCTAV

procedure.

Of the actions carried out in this procedure and of the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: On July 21 and 28, 2021 and August 26, 2021, the party

Respondent sent emails to multiple recipients without having

used the blind copy functionality, leaving email addresses visible

personal email.

SECOND: On May 11, 2022, the claimant filed a

claim before the Spanish Data Protection Agency for having received

several emails, the last one dated August 26, 2021, sent

to a plurality of recipients without having used the blind carbon copy functionality,

leaving their personal email addresses visible.

FUNDAMENTALS OF LAW

Yo

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/22

In accordance with the powers that article 58.2 of the RGPD grants to each authority of

control and as established in articles 47, 48.1, 64.2 and 68.1 of the LOPDGDD,

The Director of the Agency is competent to initiate and resolve this procedure

Spanish Data Protection.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Data Protection Agency will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

First, the claimed party acknowledges its responsibility, requesting the

20% reduction in the amount of the penalty provided for in the regulations.

Article 85.1 of the LPACAP states that "Once a disciplinary procedure has been initiated, if

the offender acknowledges his responsibility, the procedure may be resolved with the

imposition of the appropriate sanction."

Therefore, the resolution of the agreement to initiate this disciplinary procedure

indicated that "In accordance with the provisions of article 85 of the LPACAP, may

acknowledge their responsibility within the term granted for the formulation of

allegations to this initiation agreement; which will lead to a reduction in

20% of the sanction to be imposed in this procedure. With the

application of this reduction, the penalty would be established at 800 euros for the

violation of article 5.1.f) of the GDPR and 400 euros for violation of article 32

of the GDPR, resolving the procedure with the imposition of this sanction (1,200

euros in total).

On the other hand, article 85.3 of the LPACAP states that the effectiveness of such reduction

"will be conditioned to the withdrawal or resignation of any action or resource in the

administrative against the sanction."

This aspect is also included in the aforementioned resolution of the agreement to start the

this disciplinary proceeding, which also states that "In the event that

choose to proceed to the voluntary payment of any of the amounts indicated

previously (1,200 euros or 900 euros), you must make it effective by depositing

in the account number ES00 0000 0000 0000 0000 0000 opened in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A., indicating

in the concept the reference number of the procedure that appears in the

heading of this document and the reason for reducing the amount to which

welcomes."

Although the claimed party has acknowledged its responsibility within the period for

make allegations to the initiation agreement, it has not been accompanied by the

withdrawal or resignation to bring any action or appeal in administrative proceedings

against the sanction, nor the payment thereof. Moreover, it presents a written statement of allegations

so that the sanction that is imposed is not pecuniary, but a warning.

II

The defendant considers that a series of considerations should have been taken into account.
mitigating factors included in article 83 of the GDPR and in article 76.2 of the
LOPDGDD.

Article 83.2 of the GDPR states that "Administrative fines will be imposed, in
depending on the circumstances of each individual case (…). When deciding to impose
an administrative fine and its amount in each individual case will be duly
into account" a series of circumstances that are listed below.

On the other hand, article 76 of the LOPDGDD states:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation
(UE) 2016/679 will be applied taking into account the graduation criteria
established in section 2 of said article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679
may also be taken into account:

(…)"

That is, both article 83.2 of the GDPR and article 76.2 of the LOPDGDD do not
mention "aggravating" or "mitigating", but simply to circumstances or
Graduation criteria for the fine, which must be taken as a starting point
for the determination of an effective, dissuasive and proportionate fine (article 83.1
of the GDPR), as has been done in the present case.

However, the defendant understands that in this case there are a number of
of mitigating factors that must be assessed:

- Article 83.2.a) of the GDPR: "the nature, seriousness and duration of the infringement,
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 damage and damages they have suffered".

In this regard, the claimed party states that "At no time has there been a purpose of harming any of the persons involved, having been a limited-range communication with a small, determined, and known number of recipients. Additionally, the level of damages is estimated as low, also taking into account that measures will be applied to mitigate the same (request to delete the mail). For this purpose, I attach as document No. 1 what called "mails between the claimant and the recipients of the mails sent by LISMARTSA".

Recital 150 of the GDPR states that "(...) This Regulation must indicate the infractions as well as the maximum limit and the criteria to establish the corresponding administrative fines, which the competent control authority must determine in each individual case taking into account all the concurrent circumstances in

him, paying particular attention to the nature, seriousness and duration of the infringement and its consequences and the measures taken to ensure compliance with the obligations imposed by this Regulation and prevent or mitigate the consequences of the offense. (…)"

That is, the circumstances regulated in article 83.2.a) of the GDPR are the point of heading for the determination of the amount of the administrative fine, then, as indicate the Directives 04/2022 of the European Committee for Data Protection on the

calculation of administrative fines in accordance with the RGPD, in its version of 12 May 2022, subject to public consultation, "Depending on the circumstances of the case, the supervisory authority may consider that the above elements increase or decrease the perceived severity. If they are not of particular relevance, they can also considered neutral.

The initiation agreement agreed that the sanction that may correspond in the present case, without prejudice to what results from the instruction, it would be one thousand euros (€1,000), for the alleged infringement of article 5.1.f) of the GDPR, typified in article 83.5.a) of the GDPR, and five hundred euros (€500), for the alleged violation of article 32 of the GDPR, typified in article 83.4.a) of the GDPR.

To establish such amount, it took into account:

1.- That, in accordance with article 83.5.a) of the GDPR, a violation of article 5.1.f) of the GDPR may be sanctioned "with administrative fines of 20,000,000 EUR maximum or, in the case of a company, an amount equivalent to 4% as maximum of the overall annual total turnover of the previous financial year, opting for the one with the highest amount"

2.- That, in accordance with article 83.4.a) of the GDPR, a violation of article 32 of the GDPR may be sanctioned "with administrative fines of 10,000,000 EUR maximum or, in the case of a company, an amount equivalent to 2% as maximum of the overall annual total turnover of the previous financial year, opting for the one with the highest amount"

3.- That in the present case, in accordance with article 83.2.a) of the GDPR, the following circumstances of graduation of the sanction concur: (i) that the data processing has been carried out within the operation of the company, (ii) the number of people affected by the sending of emails without using the blind carbon copy functionality, (iii) that the damage caused to such persons has been the

loss of availability of your email address as it has been accessible

to third parties without your consent, who could make use of the

same without any control by its owner.

On the other hand, we cannot share the thesis of the defendant regarding the fact that the

recipients of the emails knew the other email addresses to the

view of the emails that the claimed party attached to its brief of

allegations to the start-up agreement as document no. 1:

- One sent from ***EMAIL.6 to ***EMAIL.7 on November 25, 2019.

- One sent from ***EMAIL.8 to “administracion iurisred” on December 3

of 2019.

- Two sent from ***EMAIL.6 to ***EMAIL.9.: one on December 6

of 2019 and another on December 16, 2019.

- Three sent from ***EMAIL.9 to ***EMAIL.10: One on the 21st of

November 2019, another on November 27, 2019 and another on November 5, 2019.

December 2019.

- One sent from ***EMAIL.6 to ***EMAIL.11 on November 27, 2019.

While the emails that have given rise to this procedure

sanction, have been the following:

- Email sent on July 21, 2021 from ***EMAIL.8 to

following recipients without using the blind copy functionality: ***EMAIL.12,

***EMAIL.13, ***EMAIL.14, ***EMAIL.10.

- Email sent on July 28, 2021 from ***EMAIL.8 to

following recipients without using the blind copy functionality: ***EMAIL.12,

***EMAIL.13, ***EMAIL.14, ***EMAIL.10, ***EMAIL.15.

- Email sent on August 26, 2021 from ***EMAIL.8 to

following recipients without using the blind copy functionality: ***EMAIL.12,

***EMAIL.13, ***EMAIL.14, ***EMAIL.10, ***EMAIL.15, ***EMAIL.16, ***EMAIL.4.

Therefore, it is concluded that the emails provided by the claimed party

do not certify that the different recipients of the emails in which the

blind carbon copy functionality, they knew all the email addresses

personal information contained therein.

- Article 83.2.b) of the GDPR: "intentionality or negligence in the infringement", therefore,

points out the defendant, "At no time has there been intentionality in

harm the claimant. If only Lismartsa could carry on

after being the claimant who held the reins of the company during a

decade."

Nor can this circumstance be considered an attenuation in the present case,

Therefore, as indicated in Directives 04/2022 of the European Committee for the Protection of

Data on the calculation of administrative fines in accordance with the GDPR, in its

version of May 12, 2022, submitted to public consultation, “the absence of

intent does not necessarily equate to a decrease in severity. In fact, the

gross negligence constitutes an increase in perceived seriousness, and in other cases the

negligence could, at best, be considered neutral. On the other hand, to

In this regard, it should be clear that, even when the infringement is unintentional,

may be considered a serious infringement, depending on the other circumstances of the

car case.”

- Article 83.2.c) of the GDPR: "any measure taken by the person responsible or in charge of the treatment to alleviate the damages and losses suffered by the interested".

In this regard, the claimed party states that "I cannot request the recipients of the emails that eliminate the emails that are the subject of this procedure, because I do not I have reported these email addresses, and the recipients communicated with LISMARTSA (with A.A.A.) through those addresses without using bcc."

For this purpose, it indicates that it attaches as document No. 2 "mails sent and received to Lismartsa, with the different emails that the claimant used at work with the

***EMAIL.4;

company computer:

***EMAIL.5"

EMAIL.1EMAIL.2;

***EMAIL.3;

It is not possible to understand the statement made by the claimed party to effects of applying to the present case the circumstance regulated in article 83.2.c) of the GDPR as mitigation, just as the objective of the emails attached as document no. 2, since in both cases it is not appreciates any measure aimed at alleviating the damages suffered by the recipients of emails sent without using the copy functionality hidden.

Furthermore, it should be noted that, contrary to what the defendant states,

In view of the documentation provided, it is not proven that the recipients of

the emails that have given rise to this disciplinary procedure, will be

communicate with the claimant through their different email addresses

personal email without using the blind carbon copy functionality.

On the other hand, the defendant alleges that it has hired a consulting firm

specialized in regulatory compliance, as well as four training courses in this regard.

But such measures:

1.- They are not aimed at alleviating the damages suffered by those affected by

sending emails showing their email addresses

personal email.

2.- These are measures taken by a data controller who acts based on the

principle of proactive responsibility, in accordance with article 5.2 and article

19 of the GDPR.

Finally, the claimed party indicates that "Currently we use the tool

Bcc but the recipient thinks that I have not informed all concerned and without

ask for authorization, forward the email to whomever it deems appropriate.", attaching emails

electronics for that purpose.

Regardless that this is not the forum to analyze the emails

sent by the claimed party as document no. 3, it should be noted that the

use of the blind carbon copy functionality currently by the responding party does not

It is a measure that will alleviate the damages suffered by people

who have had their email addresses improperly exposed

personal, therefore it cannot be considered a regulated circumstance in the

Article 83.2.c) of the GDPR as mitigation.

- Article 83.2.e) of the GDPR: "any previous infringement committed by the person in charge or the

person in charge of the treatment", then, points out the claimed party, that "As of the date of the

present writing, this entity has not had any sanction in terms of protection

of personal data."

Regarding the absence of a history of previously committed infractions,

the Judgment of the National Court, of May 5, 2021, rec. 1437/2020, we

provides the answer: "He considers, on the other hand, that it must be appreciated as

mitigating the non-commission of a previous infraction. Well, article 83.2 of the

GDPR establishes that it must be taken into account for the imposition of the fine

administrative, among others, the circumstance "e) any previous infraction committed by the

controller or processor". This is an aggravating circumstance,

the fact that the budget for its application does not exist implies that it cannot

be taken into consideration, but it does not imply or allow, as the plaintiff claims, her

application as mitigation".

Furthermore, Directives 04/2022 of the European Committee for the Protection of

Data on the calculation of administrative fines in accordance with the GDPR, in its

version of May 12, 2022, submitted to public consultation, indicate that "the

absence of previous infringements cannot be considered a mitigating factor, as

that GDPR compliance is the norm. If there are no prior violations, this

factor can be considered neutral.

- Article 83.2.f) of the GDPR: "the degree of cooperation with the control authority with

in order to remedy the infringement and mitigate the possible adverse effects of the

infringement".

The defendant considers that this mitigation concurs because "This part has been
fully cooperated with this control authority, and assumes the total
commitment to keep it that way throughout the procedure. between services
contracted, there is also advice on procedures before the authority
control, so they will accompany us in all the measures that this authority
deems necessary to apply."

For this purpose, it is necessary to take into account the Guidelines 04/2022 of the Committee
European Data Protection Committee on the calculation of administrative fines with
according to the RGPD, in its version of May 12, 2022, submitted to public consultation,
which state that "it must be considered that the ordinary duty of cooperation is
mandatory and therefore should be considered neutral (and not a mitigating factor)."

This is confirmed in the CEPD Guidelines on the application and
setting of administrative fines for the purposes of Regulation 2016/679, adopted on 3
of October 2017, in which it is stated that "That said, it would not be appropriate to have
In addition, take into account the cooperation that the law requires; For example, in any case
requires the entity to allow the control authority access to the facilities to
conduct audits or inspections.

- Article 83.2.g) of the GDPR: "The categories of personal data affected
for the infringement", then, indicates the defendant, that "they have only seen
affected the data of the email (...)".

Going back to the Guidelines 04/2022 of the European Committee for the Protection of

Data on the calculation of administrative fines in accordance with the GDPR, in its

version of May 12, 2022, submitted to public consultation, we find that these

state that "Regarding the requirement to take into account the categories of data

data subjects (Article 83, paragraph 2, letter g) of the GDPR), the GDPR highlights

clearly the types of data that deserve special protection and, therefore, a

stricter response in terms of fines. This refers, at least, to the

types of data contemplated in articles 9 and 10 of the GDPR, and to data that does not

fall within the scope of these articles whose dissemination causes damage or

immediate difficulties to the data subject (for example, location data, data on

private communications, national identification numbers). In general, how much

the more of these categories of data concerned or the more sensitive the data, the more serious it is

the infraction."

For these reasons, it cannot be considered a circumstance regulated in article

83.2.g) of the GDPR as mitigation of the fact that the only personal data that has been

affected is the email address.

- Article 76.2.a) of the LOPDGDD: "The continuing nature of the infringement.", therefore,

points out the defendant "This is a totally punctual infringement and

exceptional, motivated by the need to maintain the operation of the company,

which included the management of payroll, having access to the accounting, return of

access keys to the headquarters, telephone devices that are not in the headquarters and are being

paying, managing rentals of company properties…"

But a specific violation of the data protection regulations of character

personal cannot be considered as a circumstance regulated in article

76.2.a) of the LOPDGDD as mitigation, since this precept refers

literally to the continuous nature of the infraction as a criterion for grading the

sanction, without room for an interpretation a sensu contrario. That is to say, when we

we find ourselves faced with an infraction that is not of a continuous nature, it cannot be

apply the aforementioned graduation criteria as mitigation for the purpose of determining the

amount of the penalty.

The reason is none other than, in the scope of the disciplinary procedure, the principle governs

of typicity, regulated in article 27 of Law 40/2015, of October 1, of Regime

Legal Department of the Public Sector (hereinafter, RJSP) whose section 4 states that "the

rules defining offenses and sanctions will not be applicable

analog." That is, there is no room for an extensive interpretation of the principles drawn from

a norm to a case not foreseen by it.

For this purpose, we can bring up the Constitutional Court Judgment 52/2003,

of March 17, which indicates that "those other

(interpretations) incompatible with the literal wording of the applicable precepts or

inadequate to the values that they are intended to protect."

On the other hand, we cannot share the statement of the defendant regarding

that in the present case there has been a "totally punctual" infringement, since there has not been

sent a single email in which the addresses have been exposed

recipients' personal email addresses, but there have been three

emails that you have sent without using the blind copy functionality, with the

consequence of the loss of confidentiality of the personal data of the address of

personal email of the recipients.

- Article 76.2.b) of the LOPDGDD: "The link between the offender's activity and the

processing of personal data.", then, points out the defendant,

"The activity of the company is cleaning, so it does not have as its main activity

the processing of personal data for the development of its economic activity."

Certainly, the main activity of the claimed party is not linked to the

processing of personal data, but this should not imply that such circumstance is

considered as a mitigating factor, but as a neutral circumstance, just as

it happened with the absence of intent and the absence of prior violations.

And we cannot forget that the protection of personal data is a right

of natural persons protected by article 18.4 of the Constitution,

Therefore, the regulatory regulations in this regard are mandatory with

regardless of whether data processing is the main activity of the company

or not, because even these entities carry out various data processing

personnel on a regular basis for the development of the operation of the entity

(payroll management, human resources management, etc).

- Article 76.2.c) of the LOPDGDD: "The benefits obtained as a consequence of the

commission of the infringement.", then, indicates the claimed party, "No

benefit from the infringement, quite the contrary, it was intended that the company would not go bankrupt

given the impossibility of managing it (…)."

Neither the lack of benefits obtained as a result of the commission of the

infraction can be considered as a mitigating criterion, in any case it would be

of a neutral circumstance, as was the case with the previous graduation criterion

analyzed.

- Article 76.2.f) of the LOPDGDD: "Affectation of the rights of minors.", all

time, indicates the claimed party, "No rights of any

minor or vulnerable group."

Once again, the fact that there are no minors affected by the actions of the requested party does not

implies that the circumstance of article 76.2.f) of the LOPDGDD must be applied

as an extenuating circumstance.

And it is that, as we indicated, in relation to the circumstance relating to the

categories of data affected (article 83.2.g) of the GDPR), that the more

categories of data are affected or the more sensitive the data, the more

strict should be the sanction, when the treatment carried out by the offender affects

rights of minors, the higher should be the amount of the fine.

IV.

The claimed party finalizes its pleadings to the initiation agreement indicating

that the penalty of warning would be more proportional to the specific case, "bearing

into account the measures adopted and the concurrent mitigating measures, as well as the situation

delicate economy in which we find ourselves."

Recital 148 of the GDPR states that "In the event of a minor infringement, or if the fine

that was likely to be imposed would constitute a disproportionate burden on a

natural person, instead of a sanction by means of a fine, a

warning."

In the present case:

- Neither the violation of article 5.1.f) of the GDPR nor that of article 32 of the GDPR are

minor infractions, but very serious and serious, respectively.

- The claimed party is not a natural person.

Therefore, the claimed party cannot be penalized with a warning.

As we indicated in the previous Legal Basis, the start-up agreement

established that "the sanction that may correspond, without prejudice to what results from

the instruction would be:

- THOUSAND EUROS (€1,000), for the alleged violation of article 5.1.f) of the GDPR,

typified in article 83.5.a) of the GDPR.

- FIVE HUNDRED EUROS (€500), for the alleged violation of article 32 of the GDPR,

typified in article 83.4.a) of the GDPR."

Article 83.5.a) of the GDPR provides that "Violations of the provisions

following will be sanctioned, in accordance with section 2, with administrative fines

EUR 20,000,000 maximum or, in the case of a company, an amount

equivalent to a maximum of 4% of the total global annual turnover of the

previous financial year, opting for the highest amount:

a) the basic principles for the treatment, including the conditions for the

consent in accordance with articles 5, 6, 7 and 9;"

While article 83.4.a) of the RGGPD establishes that "Violations of the

following provisions will be sanctioned, in accordance with section 2, with fines

administrative costs of a maximum of EUR 10,000,000 or, in the case of a company, of

an amount equal to a maximum of 2% of the total annual turnover

of the previous financial year, opting for the highest amount:

a) the obligations of the controller and the person in charge under articles 8, 11, 25 to

39, 42 and 43; (…)"

Therefore, an administrative fine of 1,000 euros, regarding the violation of article 5.1.f) of the GDPR, and 500 euros, with respect to the violation of article 32 of the GDPR, is in the lower section of the possible sanctions, thus complying with what provided in article 83.1 of the GDPR: "Each control authority will guarantee that the imposition of administrative fines in accordance with this article for infringements of this Regulation indicated in sections 4, 5 and 6 are in each individual case, effective, proportionate and dissuasive."

However, the claimed party considers that the sanction is not proportional "taking into account the measures adopted and the concurrent mitigating measures, as well as the situation delicate economy in which we find ourselves."

In the previous Legal Basis we have already indicated that the measures adopted are typical of a data controller who acts on the basis of the principle of proactive responsibility, as well as that the extenuating factors alleged by the claimed part.

On the other hand, "the delicate economic situation" in which the defendant says that found, has not been duly accredited. And it is that the Guidelines 04/2022 of the European Data Protection Committee on the calculation of administrative fines in accordance with the GDPR, in its version of May 12, 2022, subject to consultation public, state that "As derived from the principle of proportionality, the authority of supervision may consider, in accordance with national law, further reduce plus the fine based on the principle of inability to pay. any reduction of this kind requires exceptional circumstances. In accordance with the Guidelines of the European Commission on the method of setting fines, there must be objective evidence that the imposition of the fine would jeopardize irremediably the economic viability of the affected company. In addition, the Risks must be analyzed in a specific social and economic context."

For all the foregoing, all the allegations made by the party are dismissed.

claimed to the initiation agreement.

V

Article 5.1.f) of the GDPR, "Principles relating to processing", establishes:

"1. Personal data will be:

f) processed in such a way as to guarantee adequate data security

personal data, including protection against unauthorized or unlawful processing and against

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

or organizational procedures (“integrity and confidentiality”).”

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

The claimed party has violated article 5.1.f) of the GDPR, having sent emails

emails to personal addresses without using the blind copy option, violating

Confidentiality in the processing of personal data.

SAW

If confirmed, the aforementioned violation of article 5.1.f) of the GDPR could lead to the

commission of one of the offenses typified in article 83.5 of the GDPR, which under

the heading "General conditions for the imposition of administrative fines",

has:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 20,000,000 or,

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

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

the highest amount:

a) the basic principles for the treatment, including the conditions for the

consent under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71, "Infractions", establishes that

"The acts and behaviors referred to in sections 4,

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

contrary to this organic law”.

For the purposes of the limitation period, article 72 of the LOPDGDD, “Infractions

considered very serious”, it indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that

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

following:

a) The processing of personal data in violation of the principles and guarantees

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

VII

The evidence that is available and the criteria for grading the amount of the

fine included in article 83.2 of the GDPR, allow setting a fine of €1,000 (one thousand

euro).

VIII

Regarding the security of personal data, article 32 of the GDPR, "Security

of the treatment”, establishes:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of processing, 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 and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

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

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the treatment.

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

take into account the risks presented by data processing, in particular as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and

have access to personal data can only process such data by following

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.

For its part, the GDPR in its article 4.12 defines the security violations of the

personal data such as "all those security violations that cause the

destruction, loss or accidental or illegal alteration of personal data transmitted,

stored or otherwise processed, or unauthorized communication or access to

said data."

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

The claimed party has violated article 32 of the GDPR, when an incident of

security in their systems allowing access to personal data, specifically to

personal email addresses, when emails are sent without using the

blind copy option, allowing access to the aforementioned data with breach

of the established measures.

It should be noted that the GDPR in the aforementioned precept does not establish a list of the

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

of treatment, but it 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 processing, probability risks

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

In addition, security measures must be adequate and proportionate to the
detected risk, noting that the determination of the technical measures and
organizational procedures must be carried out taking into account: pseudonymization and encryption, the
ability to ensure 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 security level,
particular account of the risks presented by data processing, such as
consequence of the destruction, loss or accidental or illegal alteration of data
personal information transmitted, preserved or processed in another way, or the communication or
unauthorized access to said data and that could cause damages
physical, material or immaterial.
In this sense, recital 83 of the GDPR states that "(83) In order to
maintain security and prevent processing from infringing the provisions of this
Regulation, the person in charge or in charge must assess the risks inherent to the
treatment and apply measures to mitigate them, such as encryption. These measures should
ensure an adequate level of security, including confidentiality, taking into account
account the state of the art and the cost of its application with respect to the risks and
the nature of the personal data to be protected. When assessing the risk in
In relation to data security, the risks involved must be taken into account.
derived from the processing of personal data, such as destruction, loss or
accidental or unlawful alteration of personal data transmitted, stored or processed
otherwise, or unauthorized communication or access to said data, susceptible
in particular of causing physical, material or immaterial damages.
In the instant case, as stated in the facts, the AEPD transferred to the party

claimed on June 27, 2022 the claim submitted for analysis,

requesting the provision of information related to the claimed incident,

confirming what was stated in the claim document by stating that "The reason for the

that the emails with Bcc are not put, it is to try to get a response from some of

the recipients to whom the mail was sent.

The liability of the claimed party is determined by the bankruptcy of

security evidenced in the claim and documentation provided, since

is responsible for making decisions aimed at effectively implementing the

appropriate technical and organizational measures to ensure a level of safety

appropriate to the risk to ensure the confidentiality of the data, restoring its

availability and prevent access to them in the event of a physical or technical incident.

IX

If confirmed, the aforementioned infringement of article 32 of the GDPR could lead to the

commission of one of the offenses typified in article 83.4 of the GDPR that under

the heading "General conditions for the imposition of administrative fines"

has:

Violations of the following provisions will be sanctioned, in accordance with the

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

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

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

the highest amount:

a) the obligations of the controller and the person in charge under articles 8, 11, 25 to

39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

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

contrary to this organic law”.

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in 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:

f) The lack of adoption of those technical and organizational measures that

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

treatment, in the terms required by article 32.1 of the Regulation (EU)

2016/679.”

x

The evidence that is available and the criteria for grading the amount of the

fine included in article 83.2 of the GDPR, allow setting a fine of €500

(five hundred euros).

eleventh

If the infringements are confirmed, it could be agreed to impose the adoption on the person responsible

appropriate measures to adjust its performance to the regulations mentioned in this

act, in accordance with the provisions of the aforementioned article 58.2.d) of the GDPR, according to the

which each control authority may "order the person responsible or in charge of the

processing that the processing operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a certain

specified term…". The imposition of this measure is compatible with the sanction

consisting of an administrative fine, according to the provisions of art. 83.2 of the GDPR.

It is noted that not meeting the requirements of this body may be

considered as an administrative offense in accordance with the provisions of the GDPR,

classified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the

opening of a subsequent administrative sanctioning procedure.

In view of the foregoing, the following is issued

PROPOSED RESOLUTION

That the Director of the Spanish Agency for Data Protection sanctions

LISMARTSA, S.L., with NIF B78112679, for the following infractions:

- From article 5.1.f) of the GDPR, typified in article 83.5.a) of the GDPR, with

a fine of €10,000 (one thousand euros).

- From article 32 of the GDPR, typified in article 83.4.a) of the GDPR, with a

fine of €500 (five hundred euros).

Likewise, in accordance with the provisions of article 85.2 of the LPACAP, you will be

informs that it may, at any time prior to the resolution of this

procedure, carry out the voluntary payment of the proposed sanction, which

It will mean a reduction of 20% of the amount of the same. With the application of this

reduction, the sanction would be established at 800 euros for the violation of article

5.1.f) of the GDPR and 400 euros for the violation of article 32 of the GDPR (1,200

euros in total), and its payment will imply the termination of the procedure. The effectiveness of

This reduction will be conditional on the withdrawal or waiver of any action or

Administrative appeal against the sanction.

In case you choose to proceed to the voluntary payment of the specified amount

above, in accordance with the provisions of the aforementioned article 85.2, you must do it

effective by entering the restricted account IBAN number: ES00 0000 0000 0000

0000 0000 (BIC/SWIFT Code: XXXXXXXXXXX) opened in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A., indicating

in the concept the reference number of the procedure that appears in the

heading of this document and the cause, for voluntary payment, of reduction of the

amount of the penalty. Likewise, you must send proof of income to the

Sub-Directorate General of Inspection to proceed to close the file.

By virtue of this, you are notified of the foregoing, and the procedure is revealed.

so that within TEN DAYS you can allege whatever you consider in your defense and

present the documents and information that it deems pertinent, in accordance with

Article 89.2 of the LPACAP.

B.B.B.

INSPECTOR/INSTRUCTOR

926-121222

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

20/22

EXHIBIT

05/11/2022 A.A.A.

06/27/2022 Transfer of the claim to LISMARTSA, S.L.

07/27/2022 Allegations of LISMARTSA, S.L.

08/11/2022 Communication to A.A.A.

09/21/2022 Agreement to start the sanctioning file against LISMARTSA, S.L.

09/21/2022 Information to A.A.A.

10/04/2022 Request for term extension from LISMARTSA, S.L.

10/06/2022 Concession of term extension to LISMARTSA, S.L.

10/19/2022 Allegations of LISMARTSA, S.L.

>>

SECOND: On February 9, 2023, the claimed party has proceeded to pay

of the sanction in the amount of 1200 euros making use of the reduction provided for in the

motion for a resolution transcribed above.

THIRD: The payment made entails the waiver of any action or resource in the

against the sanction, in relation to the facts referred to in the

resolution proposal.

FUNDAMENTALS OF LAW

Yo

Competence

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 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 Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Data Protection Agency will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

Termination of the procedure

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

The procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction has only a pecuniary nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature but the

inadmissibility of the second, the voluntary payment by the presumed perpetrator, in

any moment prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the offence.

3. In both cases, when the sanction is solely pecuniary in nature, the

The competent body to resolve the procedure will apply reductions of at least

20% of the amount of the proposed penalty, these being cumulative among themselves.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure EXP202206966, in

in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to LISMARTSA, S.L.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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 for in article 46.1 of the

referred Law.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es