☐ File No.: PS/00493/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Ms. A.A.A. and D.B.B.B. (hereinafter, the CLAIMANTS) dated

On April 21, 2021, they filed a claim with the AEPD. The claim is directed

vs. D.C.C.C. with NIF ***NIF.1 (hereinafter, the CLAIMED party).

The grounds on which the claim is based are as follows:

The CLAIMANT parties state that a security breach has occurred

caused by the sending of an email without a blind copy by the party

CLAIMED, being its content accessible to third parties.

The CLAIMING parties state that they have no relationship with the other

email recipients.

Regardless of the email addresses and the existing controversy,

reveal the names and surnames of those affected, as well as the address where

Your home is located under construction.

Together with the claim, a copy of the message sent by the claimed party is provided,

date December 29, 2020.

SECOND: In view of the facts denounced in the claim and the

documents provided by the claimant, said claim was transferred to the

RESPONDENT, to proceed with its analysis and inform this Agency in

within a month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

The notification of the transfer of the claim was carried out, by post at the address

known to the claimant, resulting in this shipment being returned by the Postal Service with

the indication "Unknown".

THIRD: On August 6, 2021, and in accordance with the provisions of the

art. 65.5 of the LOPDGDD, the claim was admitted for processing

filed by the CLAIMING parties.

FOURTH: On September 10, 2021 and in response to the request of

information sent by the General Subdirectorate of Data Inspection, has

entry in this Agency written by the claimed person in which he states the following:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

☐ Sending the email on December 29, 2020 to several

recipients has been intended to inform recipients of the

resolution of the contract of the contracted work with the claimants.

☐ It states that all recipients are related, being the pro-

pio claimed the link.

☐ In the same letter of response, list the recipients of the email

and the existing relationship with each one, identifying at least nine of

them as owners of other works in which they provide their services and

which, as stated, share an architect and/or electrical installer.

☐ Provide a copy of the Record of Customer Treatment Activities

Potentials, treatment in which the sending of the electronic mail is circumscribed.

tronic.

☐ Declares that he has not considered that the shipment made constituted a

security breach; and for this reason has not carried out the requirements

procedures established by the RGPD regarding security breaches in

its articles 33 and 34.

 States that the procedure for sending mail has changed when

are addressed to multiple recipients consisting of using the op-

tion offered by the email application through the field

known as "blind copying" (BCC) and who has received training on

the risks of using email, has been documented with the

tools published by INCIBE (for example, its blog deals with

this theme "CCO, the (still) great unknown" or "Decalogue of medi-

email security

 Considers it appropriate to take into consideration the following circumstances:

circumstances:

a) The isolated nature of the possible infraction.

b) It is not a mass mailing to potential customers.

c) The acknowledgment of the facts, without any intention

(fraud) and the lack of recidivism.

d) It does not send emails, not even for commercial purposes.

promotional or advertising of its activity or services (absent

marketing purpose)

e) The linking of its activity with the performance of treatment

personal data.

f) The invalidity of benefits obtained as a result of the

commission of the possible infraction, which was only carried out for

of transparency with the parties involved.

g) The non-affectation of the rights of minors or the treatment

special category data (only email addresses)

electronic mail).

h) It is a self-employed professional.

FIFTH: On December 22, 2021, the Director of the Spanish Agency for

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

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

of the Common Administrative Procedure of the Public Administrations (in

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

hereinafter, LPACAP), for the alleged infringement of articles 5.1.f) and 32 of the RGPD,

typified in articles 83.5 and 83.4 of the RGPD.

SIXTH: Having been notified of the aforementioned initiation agreement, the party complained against filed a written

allegations in which, in summary, it ratifies what was stated in its previous brief

presented on September 10, 2021 and states that it recognizes

expressly that the established legal precepts have been infringed, for not using

the option offered by the email application through the known field

as «blind copy» (BCC), to be able to make a shipment without showing the

email addresses of all of them; although it is true that it was done without any intention of

cause any damage to the recipients of the email.

Sending the email on December 29, 2020 to several recipients,

although it was done intentionally to inform said recipients of the

resolution of the work contract contracted with the CLAIMING party, in no

moment would influence his condition as director of execution of his works, acting with

the strictest professionalism despite the fact that the electrical installer of these works was

the now CLAIMANT, giving the go-ahead to his work if he complied correctly

with his mission, regardless of the controversies that arose in his work on C/

Almond trees 18.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

FACTS

FIRST: On December 29, 2020, an email was sent without a copy

hidden by the CLAIMED party, its content being accessible to third parties.

SECOND: The RESPONDENT party expressly acknowledges that the

established legal precepts, for not using the option offered by the application of

email through the field known as "blind copy" (BCC), to

being able to make a shipment without showing the email addresses of all of them.

It is manifested by the CLAIMED party that the shipping procedure has changed

mail when they are addressed to multiple recipients consisting of using the

option offered by the email application through the known field

as a "blind copy" (BCC) and that you have received training on the risks of using the

email, has been documented with the tools published by INCIBE

(for example, your blog deals with this topic "CCO, the (still) great unknown" or

"Decalogue of security measures in electronic mail".

FOUNDATIONS OF LAW

Yo

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

General Data Protection, hereinafter RGPD), grants each authority of

control and according to the provisions of articles 47 and 48.1 of Organic Law 3/2018, of

C/ Jorge Juan, 6

December 5, Protection of Personal Data and guarantee of rights

(hereinafter, LOPDGDD), is competent to initiate and resolve this

procedure the Director of the Spanish Data Protection Agency.

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

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

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

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures."

II

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

Common of the Public Administrations establishes in relation to the termination in

sanctioning procedures that:

"Once a sanctioning procedure has been initiated, if the offender acknowledges his responsibility,

may resolve the procedure with the imposition of the appropriate sanction".

III

In accordance with the evidence available at the present time of the

sanctioning procedure, it is considered that the proven facts constitute

of infraction.

The defendant is accused of committing an infraction for violation of the

Article 5.1.f) of the RGPD, which states that:

"1. The personal data will be:

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

including protection against unauthorized or unlawful processing and against

your transcript.

The infringement is typified in Article 83.5.a) of the RGPD, which considers as such:

"the basic principles for treatment, including the conditions for the

consent under articles 5, 6, 7 and 9".

IV

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

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

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

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

v

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established by article 83.2 of the RGPD:

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 the

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

such as the number of interested parties affected and the level of damages that

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 person in charge or of the person in charge of the treatment,

taking into account the technical or organizational measures that they have applied under

of articles 25 and 32;

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

f) the degree of cooperation with the supervisory authority in order to remedy 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 whether the person in charge or the person in charge notified the infringement and, if so, in what

measure;

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

previously against the person in charge or the person in charge in question in relation to the

same matter, compliance with said measures;

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

certification approved in accordance with article 42,

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

such as financial benefits obtained or losses avoided, directly or

indirectly, through the infringement."

SAW

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

infringement of article 5.1 f) to the claimed party, as responsible for the aforementioned

infringement typified in article 83.5 of the RGPD, and estimated the allegations

filed by the respondent, due to the circumstances of the case, it is appropriate to graduate

the fine taking into account the following mitigating factors:

. The scant link between the professional activity carried out with the treatment of

personal data.

. Measures taken to avoid future damages: modification of the

procedure for sending mail when they are addressed to multiple recipients

consisting of using the option offered by the email application through

of the field known as "blind copying" (BCC) and receiving training on the

risks of using email, documenting yourself with the tools

published by INCIBE (for example, their blog deals with this topic "CCO, the (still)

great unknown" or "Decalogue of security measures in electronic mail".

Considering the exposed factors, it is appropriate to direct a WARNING by

infringement of article 5.1 f) of the RGPD.

7th

In accordance with the evidence available at the present time of the

sanctioning procedure, it is considered that the proven facts constitute

of infraction.

The defendant is accused of committing an infraction for violation of the

Article 32 of the RGPD, which states that:

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

nature, scope, context and purposes of the treatment, as well as risks of probability

variable and seriousness for the rights and freedoms of natural persons, the responsible

The controller and the data processor will apply appropriate technical and organizational measures.

to guarantee a level of security appropriate to the risk, which, where appropriate, includes

yeah, 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 the availability and access to personal 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

I lie.

2. When evaluating the adequacy of the security level, particular account shall be taken

ta the risks that the treatment of data presents, in particular as a consequence

of the accidental or unlawful destruction, loss or alteration of personal data transmitted

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

two to said data.

3. Adherence to a code of conduct approved under article 40 or to a mechanism

certification body approved under article 42 may serve as an element for

demonstrate compliance with the requirements established in section 1 of this

Article.

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

Any person acting under the authority of the person in charge or the person in charge and having

access to personal data can only process said data following instructions

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

the Member States".

viii

This infraction can be sanctioned with a fine of €10,000,000 maximum 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

of greater amount, in accordance with article 83.4 of the RGPD.

IX

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established by article 83.2 of the RGPD:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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 the

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

such as the number of interested parties affected and the level of damages that

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 person in charge or of the person in charge of the treatment,

taking into account the technical or organizational measures that they have applied under

of articles 25 and 32;

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

f) the degree of cooperation with the supervisory authority in order to remedy 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 whether the person in charge or the person in charge notified the infringement and, if so, in what

measure;

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

previously against the person in charge or the person in charge in question in relation to the

same matter, compliance with said measures;

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

certification approved in accordance with article 42,

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

such as financial benefits obtained or losses avoided, directly or

indirectly, through the infringement."

X

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

infringement of article 32 of the RGPD to the claimed party, as responsible for the

cited infringement typified in article 83.4 of the RGPD, and estimated the allegations

filed by the respondent, due to the circumstances of the case, it is appropriate to graduate

the fine taking into account the following mitigating factors:

. The scant link between the professional activity carried out with the treatment of

personal data.

. Measures taken to avoid future damages: modification of the

procedure for sending mail when they are addressed to multiple recipients

consisting of using the option offered by the email application through

of the field known as "blind copying" (BCC) and receiving training on the

risks of using email, documenting yourself with the tools

published by INCIBE (for example, their blog deals with this topic "CCO, the (still)

great unknown" or "Decalogue of security measures in electronic mail".

Considering the exposed factors, it is appropriate to direct a WARNING by

infringement of article 32 of the RGPD.

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: SEND A WARNING to D.C.C.C. with NIF ***NIF.1, for the

infringements of articles 5.1.f) and 32 of the RGPD, typified in articles 83.5 and

83.4 of the GDPR.

SECOND: NOTIFY this resolution to Ms. A.A.A. and D.B.B.B..

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.

938-270122

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es