 File No.: EXP202104139

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the complaining party) dated September 28,

2021 filed a claim with the Spanish Data Protection Agency. The

claim is directed against JAÉN SENTIDO Y COMÚN with NIF G23798606 (in

hereinafter, the claimed party or JSyC). The grounds on which the claim is based are

following:

The claimant states that on 09/26/2021 he received an email

sent to 241 recipients with the addresses of all of them visible, without having

made use of the "blind copy BCC" functionality. Along with the writing of

claim provides a copy of the communication received, sent by JAÉN, SENTIDO Y

COMMON convening the open meeting dated 09/30/2021 of JSy C.

On 09/28/2021, the claimant addresses the political formation, requesting that

prove the authorization for the use of that email for these communications

because their participation in the municipal group was in XXXX in the process of

candidacies for mayor in which several political organizations concurred, and

You suspect that a treatment or transfer of data could have occurred without your consent.

authorization. He also requested the means of contact with the DPD.

He states that he has received an evasive answer and that he is informed that

proceeded to remove your email address from their mailing list.

contacts.

The claimant states that he requested information on the treatment carried out with his

email and no response.

Along with the claim, a copy of the e-mail sent is provided, containing

241 recipients with the addresses of all of them visible.

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

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

hereinafter LOPDGDD), said claim was transferred to the party

claimed/ALIAS, to proceed with its analysis and inform this Agency in the

period of one month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

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 not collected by the person in charge; reiterating the

transfer on 12/01/2021 by certified mail, it was returned again

for "absent".

No response has been received to this transfer letter.

THIRD: On December 23, 2021, in accordance with article 65 of

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

FOURTH: On March 18, 2022, the Director of the Spanish Agency for

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

for the alleged infringement of Article 5.1.f) of the RGPD and Article 32 of the RGPD,

typified in Article 83.4 of the RGPD.

FIFTH: Notification of the aforementioned start-up agreement in accordance with the rules established in Law 39/2015, of October 1, on the Common Administrative Procedure of the Public Administrations (hereinafter, LPACAP) and after the term granted for the formulation of allegations, it has been verified that no allegation has been received any by the claimed party.

Article 64.2.f) of the LPACAP - provision of which the respondent was informed in the agreement to open the procedure - establishes that if no allegations within the stipulated period on the content of the initiation agreement, when it contains a precise statement about the imputed responsibility, may be considered a resolution proposal. In the present case, the agreement beginning of the sanctioning file determined the facts in which the imputation, the infraction of the RGPD attributed to the claimed and the sanction that could prevail. Therefore, taking into consideration that the respondent has not formulated allegations to the agreement to initiate the file and in attention to what established in article 64.2.f) of the LPACAP, the aforementioned initial agreement is considered in this case proposed resolution.

In view of everything that has been done, by the Spanish Data Protection Agency In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: A.A.A. (hereinafter, the complaining party) dated September 28, 2021 filed a claim with the Spanish Data Protection Agency. The claim was directed against JAÉN SENTIDO Y COMÚN with NIF G23798606 (in hereinafter, the claimed party or JSyC). The grounds on which the claim is based are following:

The claimant on 09/26/2021 received an email sent to 241

recipients with the addresses of all of them visible, without having used the

"blind copy BCC" functionality. Along with the written claim, provide

copy of the communication received, sent by JAÉN, SENTIDO Y COMÚN

convening the open assembly dated 09/30/2021 of JSy C.

On 09/28/2021, the claimant addressed the political formation, requesting that

accredit the authorization for the use of that email for these communications

because their participation in the municipal group was in XXXX in the process of

candidacies for mayor in which several political organizations concurred, and

You suspect that a treatment or transfer of data could have occurred without your consent.

authorization. He also requested the means of contact with the DPD.

The claimant received an evasive answer in which he was informed that

proceeded to remove your email address from their mailing list.

contacts.

The claimant requested information on the treatment carried out with his email

email and have not received a response.

FOUNDATIONS OF LAW

Yo

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

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

control authority and as established in articles 47 and 48.1 of the Law

Organic 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 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

The facts denounced are specified in the sending of a call for Assembly to

a series of recipients, without hiding their respective email addresses

electronically, violating the principle of confidentiality.

Said treatment could constitute an infringement of article 5 of the RGPD,

Principles relating to processing, which states that:

"1. The personal data will be:

(…)

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

personal data, including protection against unauthorized or unlawful processing and

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

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

(…)”

The documentation in the file offers clear indications that the party

claimed violated article 5 of the RGPD, principles related to treatment, by disclosing

to third parties, personal data (specifically the email address),

by submitting a meeting call without a blind copy. This is due to the lack of

adequate security measures, as motivated in the following section.

III

Article 32 of the RGPD, security of treatment, establishes the following:

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

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

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

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

which in your case includes, among others:

pseudonymization and encryption of personal data;

the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

b) a process of regular verification, evaluation and evaluation 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 shall be given to

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

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data (The underlining is from the AEPD).

Recital 75 of the RGPD lists a series of factors or assumptions associated with

risks for the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and

variable probability, may be due to the processing of data that could cause

physical, material or non-material damages, particularly in cases where

that the treatment may give rise to problems of discrimination, usurpation of

identity or fraud, financial loss, reputational damage, loss of

confidentiality of data subject to professional secrecy, unauthorized reversal of the

pseudonymization or any other significant economic or social damage; in the

cases in which the interested parties are deprived of their rights and freedoms or are

a)

b)

a)

prevent exercising control over your personal data; In cases where the data

treated personalities reveal ethnic or racial origin, political opinions, religion

or philosophical beliefs, militancy in trade unions and the processing of genetic data,

data relating to health or data on sex life, or convictions and offenses

criminal or related security measures; In cases where they are evaluated

personal aspects, in particular the analysis or prediction of aspects related to the

performance at work, economic situation, health, preferences or interests

personal, reliability or behavior, situation or movements, in order to create or

use personal profiles; in the cases in which personal data of

vulnerable people, in particular children; or in cases where the treatment

involves a large amount of personal data and affects a large number of

interested."

The facts revealed mean that it is not accredited in the file

the existence of adequate technical and organizational measures in accordance with what is required in

the RGPD, when disclosing information and personal data to third parties, with the

consequent lack of diligence by the person in charge, having sent an email

without blind copy to 241 recipients, thus facilitating each recipient the

access to the email of the rest of the recipients, which supposes a

disclosure of personal data to third parties.

IV

Article 4.12 of the RGPD establishes that it is considered “violation of the security of the

personal data: any breach of security that results in the destruction, loss

or accidental or unlawful 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

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

security, by sending an email without a blind copy to 241 recipients, among

them the claimant, in which an Assembly is convened, disclosing information and

personal data to third parties.

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

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

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

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

the treatment, taking into account the state of the art, the application costs, the

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

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

Likewise, the security measures must be adequate and proportionate to the

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

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

capacity to guarantee confidentiality, integrity, availability and resilience, the

ability to restore availability and access to data after an incident, process

verification (not audit), evaluation and assessment of the effectiveness of the

measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such as

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

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

“(83) In order to maintain security and prevent the treatment from violating the provisions of

this Regulation, the person in charge or the person in charge must evaluate the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. These

measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

Article 83.5 of the RGPD provides the following:

v

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

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

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

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

the largest amount:

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

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

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what

following: "The acts and behaviors referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law."

Establishes article 72 of the LOPDGDD, under the rubric of infractions considered

very serious, the following: "1. Based on the provisions of article 83.5 of the

Regulation (EU) 2016/679 are considered very serious and will expire after three years

infractions that suppose a substantial violation of the articles

mentioned therein and, in particular, the following:

(…)

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

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

The violation of article 32 RGPD is typified in article 83.4.a) of the

cited RGPD in the following terms:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/9

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

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

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

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

the largest amount:

a) the obligations of the person in charge and the person in charge in accordance with articles 8, 11,

25 to 39, 42 and 43."

(…)

It establishes article 73 of the LOPDGDD, under the heading "Infringements considered

serious", the following:

"Based on the provisions of article 83.4 of Regulation (EU) 2016/679,

considered serious and will prescribe after two years the infractions that suppose a

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

following:

(…)

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

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679.

In the present case, the infringing circumstances provided for in article

SAW

This infringement of article 32.1. of the RGPD can be sanctioned with a fine of

A maximum of 10,000,000.00 euros or, in the case of a company, an amount

equivalent to a maximum of 10% of the total global annual turnover of the

previous financial year, opting for the highest amount, in accordance with the

article {83.4, of the RGPD.

This infringement of article 5.1.f) of the RGPD can be sanctioned with a fine of

20,000,000.00 euros maximum or, in the case of a company, an amount

equivalent to a maximum of 20% of the total global annual turnover of the

previous financial year, opting for the highest amount, in accordance with the

article 83.5 of the RGPD.

7th

The text of the resolution establishes the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of

data, from which it is clearly inferred what measures to adopt for their

fix (configuring mail delivery so that it can be sent with

hidden copy when addressed to a plurality of interested parties), notwithstanding that the

type of procedures, mechanisms or specific instruments to implement them

corresponds to the sanctioned party, since it is the data controller who

fully knows your organization and has to decide, based on the responsibility

proactive and risk-focused, how to comply with the RGPD and the LOPDGDD.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE JAÉN SENIDO Y COMÚN, with NIF G23798606, one:

- Penalty of 500 euros (five hundred euros), for the violation of article 32.1 of the RGPD,

typified in article 83.4 of the RGPD and considered "serious" for the purposes of prescription

in article 73.f) of the LOPDGDD.

- Penalty of 1,500 euros (one thousand five hundred euros), for the infraction of article 5.1.f) of the

RGPD, typified in article 83.5 of the RGPD and considered "very serious" for the purposes of

prescription, in article 72.1.a) of the LOPDGDD.

SECOND: REQUIRE, by virtue of the corrective powers that article 58.2 of the

RGPD grants to the control authorities, that the person in charge configures the sending of

emails so that they can be blind-copied when addressed to a

plurality of interested party, as a measure that should be adopted so that the

infringing conduct analyzed, the effects of the infraction committed are corrected and

adapt the treatments to the requirements contemplated in articles 5.1.f) and 32 of the

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

required, within 10 business days from the day after receipt of the

notification of this resolution.

THIRD: NOTIFY this resolution to JAÉN SENTIDO Y COMÚN.

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, on Administrative Procedure

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

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

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

Otherwise, it will be collected in the executive period.

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

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following month or immediately after, and if

between the 16th and last day of each month, both inclusive, the payment term

It will be until the 5th of the second following month or immediately after.

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

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the

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

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

938-050522

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es