 File No.: PS/00571/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant), dated January 3,

2021, filed with the Spanish Data Protection Agency, a claim against

the CITY COUNCIL OF FUENLABRADA, with NIF P2805800F (hereinafter, the

TOWN HALL).

The complaining party informs this Spanish Agency for the Protection of

Data that the CITY COUNCIL has sent an email "without a blind copy" to

a plurality of people registered in the "Municipal list of XXXXXX", as well as that

In said email a document was attached that included a list with the

personal data (name, surnames, and DNI) of these people.

Along with the claim, provide:

- Copy of the email addressed by the claimed party (the origin of the email

entered therein would correspond to the name and surnames of the

employee of the respondent who would have sent it) to those affected (includes, within

of the “To” section a set of email addresses) dated

of November 20, 2020.

The subject of the email is "Consultation of the pre-list of beneficiaries

Municipal Bank of XXXXXX”.

The body of the message contains, among others, the following paragraphs:

“I send you the list that has been notified to us by Civil Protection in which

All the people who have finally carried out some activity are listed.

of BMT until November 10.

I would like to ask you, please, to consult it and if there was someone who hu-

had carried out the activity and did not appear on said list, was put in

Contact me by email referring me to such incident, to

be able to solve it.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/11

[…] This preliminary list is not the resolution of the file, with what would have to be

Wait for the approval of the file in the Local Government Board and its publication.

tion to carry out the income of the amounts of BMT.”

In addition, the review of containing an attachment with the title "List of Students" is included.

day…day.pdf”.

- Copy of the document attached to the email described in the previous point.

The document includes a list of people for each of whom

They require the following values: “ORDER LIST”, “UNIVERSITY NAME”,

“SURNAME 1”, “SURNAME 2”, “DNI”.

SECOND: On February 12, 2021, and in accordance with the provisions of the

Article 65.4 of Organic Law 3/2018, of December 5, on Data Protection

Personal and guarantee of digital rights (hereinafter LOPDGDD) is given

transfer of said claim to the claimed party, so that it could proceed with its analysis

and inform this Agency within a month of the actions carried out

to adapt to the requirements set forth in the data protection regulations.

On March 4, 2021, this Agency records a response to the transfer of the

claim, admitting the claim filed by the claimant

by agreement dated March 22 of that same year.

As a result of the transfer of the claim and the request for referral of

information, the CITY COUNCIL was aware of the data security breach

suffered, proceeding to notify the Spanish Protection Agency

of data.

THIRD: On February 24, 2021, the Subdirectorate General for Inspection

of Data received for its assessment a security breach notification letter

of the personal data sent by the CITY COUNCIL, received on the 17th of

February 2021, of which he is aware when he is transferred from the

claim filed by the claimant.

For the appropriate purposes, the Spanish Data Protection Agency is informed of

the next:

(...).

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts

of the notification, having knowledge of the following extremes:

(...).

Prior to the incident, the CITY COUNCIL before the implementation of the

RGPD and from its application (...).

Immediately after becoming aware of the request for information from the

AEPD, after the presentation of the claim, (...):

either (…).

FIFTH: On January 5, 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 articles 5.1 f), 32 and 33 of the RGPD, typified in the

articles 83.5 and 83.4 of the RGPD.

SIXTH: The CITY COUNCIL, on January 21 of this year, submitted a written

of allegations to the initial agreement, in which it states the following:

FIRST. – (…).

The fact that there is no record of a subsequent use of the personal information

disseminated does not distort the fact that there has been an unauthorized access

authorized email addresses of all participants in

the "Banco del XXXXXX" program, as well as the Word document, which is

attached, with their names, surnames and DNI/NIE or passport numbers,

violating the principle of confidentiality.

It is understood that the security measures implemented were insufficient,

likely to be improved; what is revealed by the statement

of the City Council that it has proceeded to the REINFORCEMENT of the policy of

security.

It is noteworthy that at the time of becoming aware of the claim,

From the Department of Data Protection, a Circular was sent with the

instructions to follow when publishing listings that carry

personal data, addressed to all employees of the City Council of

Fuenlabrada, Autonomous Organizations and Municipal Companies as well as a

second circular, also to all employees, to remember certain issues

fundamentals related to treatments in which they are involved

personal data, ensuring that the information reaches the

all those interested so that it is put into practice and there are no

omissions due to ignorance in future actions.

Accordingly, the claims were DISMISSED.

SECOND. – (…).

The CITY COUNCIL, as data controller, is obliged

to apply the appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk presented by the data processing.

These measures are not only measures of computer systems but also

human factor organizational measures.

Article 32 of the RGPD does not establish a list of security measures

that are applicable according to the data that are the object of

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

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

risk involved in the treatment, taking into account the state of the art,

the costs of application, the nature, scope, context and purposes of the

treatment, the risks of probability and seriousness for the rights and

freedoms of the persons concerned.

Likewise, the security measures must be adequate and

proportionate to the detected risk, pointing out that the determination of the

technical and organizational measures must be carried out taking into account: the

pseudonymization and encryption, the ability to ensure confidentiality,

integrity, availability and resiliency, the ability to restore the

availability and access to data after an incident, verification process (which

no audit), evaluation and assessment of the effectiveness of the measures.

In any case, among the measures cited in relation to the system of

implementation of data processing we must highlight the obligation to

the same in compliance with current regulations on protection

of data.

Accordingly, the claims were DISMISSED.

THIRD. – (…).

Even in the case of not publishing an administrative act in the terms

provided for in article 45 of Law 39/2015, of October 1, of the

Common Administrative Procedure, we can affirm that the receivers

of said email as participants of the “Banco del

XXXXXX”, were part of a group of users who voluntarily joined

they had enrolled; although, at no time, did they give their consent to

share the information disseminated in said email.

In no case, the fact that it is not an administrative procedure or the

neither urgency nor haste justify unauthorized access to the information disseminated

through an email.

If there was a risk that public employees would send emails to

administered without a blind copy had not been taken by the City Council

any technical warning measures in order that the sending of said

emails comply with the principle of confidentiality legally

required. Among the measures provided, there was none that mentioned

this risk and the measures to implement.

Consequently, we could only speak of a human error, punctual and

independently if such technical warning measure had been

sent the email without a blind copy.

Accordingly, the claims were DISMISSED.

SEVENTH: On April 8, 2022, a resolution proposal was formulated,

proposing:

IMPOSE the CITY COUNCIL OF FUENLABRADA, with NIF P2805800F, for a

infringement of Article 32 of the RGPD, typified in Article 83.4 of the RGPD, a

warning sanction.

IMPOSE the CITY COUNCIL OF FUENLABRADA, with NIF P2805800F, for a

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

warning sanction.

IMPOSE the CITY COUNCIL OF FUENLABRADA, with NIF P2805800F, for a

infringement of Article 33 of the RGPD, typified in Article 83.4 of the RGPD, a

warning sanction.

EIGHTH: The proposed resolution was attached as an annex to the list of

documents involved in the procedure.

NINTH: Once the proposed resolution has been notified and the term for it has elapsed, no

It is known that new allegations have been filed by the CITY COUNCIL.

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: It is accredited that the CITY COUNCIL has disseminated personal data

of the complaining party without his consent.

SECOND: It is accredited that the CITY COUNCIL has sent an email

“no blind copy” electronic mail to a plurality of people registered in the “list

Municipal del XXXXXX”, as well as that in said e-mail was attached a

document that included a list with personal data (name, surnames, and DNI)

of these people.

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

Article 5.1.f) of the RGPD

Article 5.1.f) “Principles related to treatment” of the RGPD establishes:

"1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational structures (“integrity and confidentiality”).”

In the present case, it is proven that there has been unauthorized access to

the email addresses of all the participants in the program “Banco

of XXXXXX”, also attaching a Word document with their names, surnames and

DNI/NIE or passport numbers, violating the principle of confidentiality; Yes

well, there is no evidence that there has been any subsequent use, by

third parties, of the personal information of none of those affected.

For this reason, the defendant is imputed the commission of an infraction by

violation of article 5.1.f RGPD.

In the present case, the security breach must be qualified as confidentiality,

as a consequence of unauthorized or illicit access to personal data of the party

claimant, due to the unauthorized sending of a writing by the party

claimed.

The data of the complaining party have been exposed without the adoption of the

necessary prior measures to avoid it, not being covered, according to the current

criteria of this body, its dissemination, for which it is considered accredited the

described offense.

Classification of the infringement of article 5.1.f) of the RGPD

III

The infringement of article 5.1.f) of the RGPD is typified in article 83.5 of the

RGPD that under the heading “General conditions for the imposition of fines

administrative” provides:

“The infractions of the following dispositions 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

of greater 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 "Infringements" establishes that

“The acts and behaviors referred to in sections 4, 5 constitute infractions.

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

to this organic law.

For the purposes of the limitation period, article 72 “Infringements considered very

serious” of the LOPDGDD indicates:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

considered very serious and will prescribe after three years the 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. (…)”

Article 32 of the RGPD establishes:

IV

“Security of treatment

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

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

variable probability and severity for the rights and freedoms of individuals

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

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure 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 account shall be taken of

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

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

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

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a certification mechanism approved under article 42 may serve as an element to demonstrate compliance with the requirements established in section 1 of the present article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that any person acting under the authority of the person in charge or the person in charge and has 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 the Right of the Union or the Member States.

It is considered that the party complained against has failed to comply with the provisions of article 32 of the RGPD, by not having the appropriate organizational and technical measures to prevent exposure of personal data.

In this regard, the CITY COUNCIL has not provided an analysis of the risk related to the sending emails without a blind copy or the existence of specific measures aimed at avoid sending to multiple recipients without using the “blind copy” functionality.

Classification of the infringement of article 32 of the RGPD

v

The infringement of article 32 of the RGPD is typified in article 83.4 of the RGPD that under the heading “General conditions for the imposition of fines administrative” provides:

“The infractions of the following dispositions 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 pursuant to articles 8,

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" 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 “Infringements considered serious”

of the LOPDGDD indicates:

“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

are appropriate to guarantee an adequate level of security when

risk of treatment, in the terms required by article 32.1 of the

Regulation (EU) 2016/679.

Article 33 of the RGPD establishes:

SAW

Article 33 “Notification of a violation of the security of personal data to

the control authority" of the RGPD establishes:

"1. In case of violation of the security of personal data, the person in charge of the

treatment will notify the competent control authority in accordance with the

article 55 without undue delay and, if possible, no later than 72 hours after

who was aware of it, unless it is unlikely that such violation

constitutes a risk to the rights and freedoms of individuals

physical. If the notification to the supervisory authority does not take place within the period of 72

hours, must be accompanied by an indication of the reasons for the delay.

2. The person in charge of the treatment will notify without undue delay the person in charge of the

treatment the violations of the security of the personal data of which it has

knowledge.

3. The notification referred to in section 1 must, at a minimum:

a) describe the nature of the data security breach

including, where possible, the categories and number

approximate number of stakeholders affected, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

4. If it is not possible to provide the information simultaneously, and to the extent that

is not, the information will be provided gradually without undue delay.

5. The data controller will document any breach of data security.

personal data, including the facts related to it, its effects and the

corrective measures taken. Said documentation will allow the authority of

control to verify compliance with the provisions of this article."

In the present case, it is known that the CITY COUNCIL suffered a security breach

of personal data on November 20, 2020; although, the

THE CITY COUNCIL was not aware of the security breach produced until the day

February 15, 2021, when you receive through the Check-in of the

CITY COUNCIL the letter of transfer of the claim that has been filed in

the AEPD.

Consequently, the CITY COUNCIL proceeded to notify the breach of

security to the AEPD, on February 17 of that same year, within the period established in the

RGPD for this purpose and with the information established in article 33 of the RGPD.

Therefore, it is considered that there is no violation of article 33 of the RGPD.

Article 83 "General conditions for the imposition of administrative fines" of the

RGPD section 7 establishes:

7th

"Without prejudice to the corrective powers of the control authorities by virtue of art.

Article 58(2), each Member State may lay down rules on whether

of, and to what extent, impose administrative fines on authorities and public bodies

public authorities established in that Member State."

Likewise, article 77 “Regime applicable to certain categories of

responsible or in charge of the treatment” of the LOPDGDD provides the following:

"1. The regime established in this article will be applicable to the treatment of

who are responsible or in charge...

c) The General Administration of the State, the Administrations of the

autonomous communities and the entities that make up the Administration

Local…

2. When those responsible or in charge listed in section 1 committed

any of the infractions referred to in articles 72 to 74 of this law

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

also the measures that should be adopted to stop the behavior or correct it.

the effects of the infraction that had been committed.

(…)

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article. (…)”

viii

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, without prejudice

that the type of specific procedures, mechanisms or instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

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

proactive responsibility and risk approach, 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 the FUENLABRADA CITY COUNCIL, with NIF P2805800F,

for an infringement of Article 32 of the RGPD, typified in Article 83.4 of the RGPD,

a warning sanction.

IMPOSE the CITY COUNCIL OF FUENLABRADA, with NIF P2805800F, for a

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

warning sanction.

SECOND: PROCEED TO FILE the present proceedings regarding the

infringement of article 33 RGPD.

THIRD: NOTIFY this resolution to the CITY COUNCIL OF

FUENLABRADA.

FOURTH:

in accordance with the provisions of article 77.5 of the LOPDGDD.

COMMUNICATE this resolution to the Ombudsman,

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

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

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

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

Interested parties may optionally file an appeal for reconsideration before the

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

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

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

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

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

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

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

aforementioned Law.

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

may provisionally suspend the firm resolution in administrative proceedings if the

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

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

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

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

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

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

documentation proving the effective filing of the contentious appeal-

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

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

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

938-050522

www.aepd.es