 File No.: EXP202207415

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: Mrs. A.A.A. (hereinafter, the claiming party) dated June 9, 2022

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the D.G. OF THE PUBLIC EMPLOYMENT SERVICE with NIF

S7800001E (hereinafter, DGSEPE).

The reasons on which the claim is based are the following:

The receipt of an email, sent from the address ***EMAIL.1 and

sent to a plurality of recipients without having made use of the functionality

BCC, allowing each of the recipients to have access to the addresses of

shipping all.

Along with the notification, a screenshot of the message is provided, dated 9/6/22.

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 forwarded to the DGSEPE, so that

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements established in the regulations of

Data Protection.

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 July 8, 2022 as

It is stated in the certificate that is in the file.

Although, no response to this letter of transfer has been received.

THIRD: On September 9, 2022, in accordance with article 65 of

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

FOURTH: On November 15, 2022, the Director of the Spanish Agency

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

for the alleged violation of Article 5.1.f) of the GDPR and Article 32 of the GDPR,

typified in Article 83.5 of the GDPR and Article 83.4 of the GDPR, respectively.

FIFTH: Notified 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

Public Administrations (hereinafter, LPACAP), the claimed party submitted a written

of allegations in which he stated:

"For all the above, the following ALLEGATIONS are formulated:

FIRST. Below is a chronological account of how the DGSPE

had knowledge of facts related to the claim that has motivated

the initiation of the disciplinary file:

A) DATA PROTECTION BREACH

June 9, 2022

The person from the DGSPE who acts as interlocutor between this center

manager and the Department of Data Protection of the Ministry (hereinafter,

DPD), is aware of a data protection breach reported by

email address of the DPD (to whom an individual –different from the claimant-

had sent an email reporting the same facts), in which

following terms:

"Attached below the complaint by email from the interested party..., copied

among the 700 or more email addresses that appear in the

copy of the email sent from (***EMAIL.1) the Unit of

Management of centralized processes of employment offices of the Sub-directorate

General Office of Employment and Employer Services (reporting on a

Office course)."

(Document “Evidence 1 Communication of security breach.msg)

June 10, 2022:

The breach is notified to the person in charge of the treatment: holder of the DGSPE.

(Document “Evidence 1 Communication of security breach.msg)

The security breach is logged in the log enabled for

this (according to the internal procedure).

A report of what happened is requested from the Sub-directorate of offices

of employment and services to the employer (Document "Evidencia2 request

security breach report.msg)

The security breach is evaluated according to the procedure

internally established, without proceeding to notify the AEPD or the

interested.

Mail is sent for diffusion between employment offices,

recalling the rules on the use of email, to which

effect, a document on "Recommendations and good

personal data protection practices for the use of mail

corporate email" approved by the Protection Working Group

of Data of the Community of Madrid (Document "Evidencia3

recommendations and good practices for the use of email

electronic.msg" and Document "Evidence 3 and 4 recommendations and

good practices PDP in use of mail V1.pdf)

Likewise, a reminder is sent to all sub-addresses of

□

this General Directorate of the Public Employment Service, recalling the

email usage rules. (Document "Evidence 4

recommendations and good practices for the use of email

for rest subaddresses.msg")

B) COMPLAINT AND REQUEST FOR INFORMATION FROM THE AEPD

July 7, 2022:

The DPD transfers to the interlocution of data protection in the Directorate

General of the Public Employment Service the notice received in the mailbox

corporate, which announced the notification sent by the AEPD to the DGSPE

for the information of the delegation.

July 8, 2022:

Notification of the AEPD is accepted at 05:00 automatically, through

of the registration application of the Community of Madrid (e-reg), in which

the notifications sent via DEHU are dumped, since the NIF of the Community

of Madrid is unique, being the one who holds the legal personality of the

that counseling is lacking.

The AEPD notification, dated July 7, 2022, consists of a

information request to the Data Controller (the DGSPE), to

purpose of the claim presented before it (referring to the breach of

confidentiality discussed above), which has given rise to this procedure

disciplinary action, as well as to be informed about the measures adopted

to avoid similar incidents and other relevant extremes, granting you

a period of one month for it.

July 21, 2022

Before exhausting the aforementioned term of the month, the Report on the

data protection breach requested in the requirement of the AEPD

(Document "Evidencia5 Preparation of report to send to the AEPD.msg" and

the PFD document attached "EXP GAP REPORT XXXXXXXX")".

In response to said allegation, this Spanish Data Protection Agency

It should be noted that the chronological account of the facts exposed; in no case,

distorts the legal classification of the facts and offenses committed.

"SECOND. Unfortunately, coinciding with other topics and with the

intention of leaving the most peremptory closed before the imminence of the

summer vacation, a fatal clerical error was made, leaving

I sent the response to said requirement despite the fact that it was elaborated and

that measures had been taken in this regard.

As an added preventative measure, it is reported that it is currently in

a plan is underway to modernize and improve the information system

called "Comprehensive Employment System", to which it is linked (among other

functionalities), sending emails informing of training courses

training (fact that caused, together with a human error, the erroneous sending of

massive without blind carbon copy). Requirements analysis is in progress

necessary for better and more controlled communication with users

to avoid these errors as much as possible.

In response to this allegation, it should be mentioned that all measures of

security measures adopted to prevent incidents such as the one that occurred between

within its obligations in compliance with data protection regulations; already

that, as the person responsible for data processing, is obliged to apply the measures

appropriate technical and organizational measures to guarantee a level of security appropriate to the

risk posed by data processing.

These measures are not only measures of computer systems but also

human factor organizational measures.

However, this organization positively values the security measures

adopted later; Although, that does not distort the commission of the aforementioned

infractions.

For all of the above, the allegations presented were DISMISSED.

SIXTH: On March 10, 2023, a resolution proposal was formulated,

proposing to sanction D.G. OF THE PUBLIC EMPLOYMENT SERVICE, with NIF

S7800001E, for a violation of Article 5.1.f) of the GDPR and Article 32 of the GDPR,

typified in article 83.5 and article 83.4 of the GDPR respectively, with a

penalty of warning for each of the infractions.

SEVENTH: Notification of the proposed resolution, in accordance with the established norms

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

Public Administrations (hereinafter, LPACAP), on March 27, 2023, the

they presented allegations by the DGSPE.

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: The receipt by the claimant of an email is accredited

email, dated June 9, 2022, sent from the address ***EMAIL.1 and

sent to a plurality of recipients (700 or more email addresses

e-mail) without having used the BCC functionality.

SECOND: It is proven that the non-use of the BCC functionality in the

sending said email allowed each of the recipients to have

access to everyone's shipping addresses.

FUNDAMENTALS OF LAW

Yo

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."

In response to the allegations presented to the motion for a resolution by the claimed entity, the following must be indicated, according to the proposed order:

II

"FIRST. The DGSPE reiterates in the chronological account presented in its previous pleadings brief, on how he learned of the facts related to the claim that has led to the initiation of the file sanction, reiterating that unfortunately on July 21, 2022, before When the deadline expired, the Report on the data protection breach was ready requested in the AEPD requirement, but an error was made administrative fatal, leaving without sending the response to said requirement to despite the fact that it was elaborated and that measures had been taken at the regard."

In response to said allegation, this Spanish Data Protection Agency It should be noted that the chronological account of the facts exposed; in no case, distorts the legal classification of the facts and offenses committed.

“SECOND The DGSPE informs of the additional measures adopted to to avoid, as much as possible, the reoccurrence of cases like this, have been the

following:

- Mail is sent for diffusion among the employment offices, reminding the

rules on the use of email, for which purpose is attached

document on "Recommendations and good practices in protection of

personal data for the use of corporate email" approved by

the Data Protection Working Group of the Community of Madrid

(Evidence 1 and 2).

- Likewise, a reminder is sent to all the sub-addresses of this

General Directorate of the Public Employment Service, recalling the rules of

use of email. (Evidence 3).

- On 03/21/2023, an official letter was sent to Mrs. B.B.B. – CEO

of the Agency for the Digital Administration of the Community of Madrid

requesting the urgent adoption of measures that prevent sending, from accounts

generic, emails to multiple users, without these being blind copies and

the need and importance of having the Automated System of

Multichannel Communication requested by this General Directorate in the project

SIE_NUBE, using all available means to expedite the

contracting and development of this system, with the purpose that the

automation of these communications eliminates the possibility of

produce human errors. (Evidence 4).

- The hiring of a tailor-made training course of 30

hours of duration aimed at DGSPE employees assigned to offices of

employment, on data protection and digital security. (Evidence 5)".

In response to said allegation, this Agency values positively all the

measures taken.

All the measures adopted allow us to affirm that the person responsible before issuing this

resolution has already adopted adequate measures to adjust its action to the

protection regulations, in accordance with the provisions of the aforementioned article 58.2 d) of the

GDPR, according to which each control authority may "order the person responsible or

processor that the processing operations comply with the

provisions of this Regulation, where applicable, in a certain way

and within a specified period…".

Consequently, the imposition of any measure in this sense will not proceed in

the present resolution.

II

Article 5.1.f) of the GDPR

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

"1. Personal data will be:

(…)

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

personal information, including protection against unauthorized or unlawful processing and against its

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

appropriate organizational procedures ("integrity and confidentiality")."

In the present case, it is clear that the personal data of the complaining party and of all

both recipients, registered in the DGSEPE database, were improperly

exposed to third parties on June 9, 2022 by sending an email

e-mail without a blind copy, your email address being accessible.

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

IV.

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

mission of the offenses typified in article 83.5 of the GDPR that under the rubric

"General conditions for the imposition of administrative fines" provides:

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

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

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

overall annual total business of the previous financial year, opting for the one with the highest

amount:

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

lien 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 are contrary to

rias to the present organic law”.

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

you see” of the LOPDGDD 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

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

Penalty for violation of article 5.1.f) of the GDPR

V

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

GDPR section 7 establishes:

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

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

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

public establishments established in that Member State.”

Likewise, article 77 “Regime applicable to certain categories of liability”

responsible or responsible for 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 State Administration, the Administrations of the communi-

autonomous entities and the entities that make up the Local Administration…

2. When the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this organic law

only, the data protection authority that is competent will issue a resolution

sanctioning them with warning. The resolution will also establish the

measures that should be adopted to cease the conduct or to correct the effects of the

offense that was committed.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

enough evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on the disciplinary or sanctioning regime that

be applicable.

Likewise, when the infractions are attributable to authorities and executives, and

accredit the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution in which the

sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or regional Gazette that

corresponds.

4. The data protection authority must be informed of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

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. (…)"

Therefore, it is appropriate to sanction the DGSEPE with a warning for the infringement

of article 5.1.f) of the GDPR,

SAW

GDPR Article 32

Article 32 "Security of treatment" of the GDPR establishes:

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

nature, scope, context and purposes of processing, as well as probability risks

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

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

measures to guarantee a level of security appropriate to the risk, which, where appropriate, will include

yeah, among others:

a) the 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 assessment of effectiveness

technical and organizational measures to guarantee the security of processing

I lie.

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

The risks presented by the data processing, in particular as a consequence

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

collected, preserved or processed in another way, or the unauthorized communication or access

two to said data.

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

certification document approved in accordance with article 42 may serve as an element to

demonstrate compliance with the requirements established in section 1 of this

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 having

ga access to personal data can only process such data following instructions

of the controller, unless it is required to do so by Union law or by

the Member States".

In the present case, at the time of the security breach, there is no record

that the DGSEPE. had reasonable security measures in place based on the

estimated possible risks.

It is evident that the DGSEPE did not use the procedure for sending emails.

e-mails when they are addressed to multiple recipients, consisting of using the option

offered by the email application through the field known as "com-

"hidden pia" (CCO), allowing each of the receivers to have in view the rest

shipping addresses; and therefore, violating the current regulations regarding

Data Protection.

Consequently, the DGSEPE did not have adequate measures to guarantee

the confidentiality, integrity and availability of processing systems and services

I lie.

Classification of the infringement of article 32 of the GDPR

VII

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

sion of the offenses typified in article 83.4 of the GDPR that under the rubric

"General conditions for the imposition of administrative fines" provides:

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

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

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

overall annual total business of the previous financial year, opting for the one with the highest

amount:

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

11, 25 to 39, 42 and 43; (…)”

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

The acts and behaviors referred to in sections 4, 5 and 6 have infractions

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

the present 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, the

They are considered serious and will prescribe after two years the infractions that suppose a vulnerability.

substantial portion of the articles mentioned therein and, in particular, the following:

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

have appropriate measures 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”. (…)

Penalty for violation of article 32 of the GDPR

VIII

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

GDPR section 7 establishes:

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

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

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

public establishments established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of liability"

responsible or responsible for 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 State Administration, the Administrations of the communi-

autonomous entities and the entities that make up the Local Administration…

2. When the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this organic law

only, the data protection authority that is competent will issue a resolution

sanctioning them with warning. The resolution will also establish the

measures that should be adopted to cease the conduct or to correct the effects of the

offense that was committed.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

enough evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on the disciplinary or sanctioning regime that

be applicable.

Likewise, when the infractions are attributable to authorities and executives, and

accredit the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution in which the

sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or regional Gazette that

corresponds.

4. The data protection authority must be informed of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

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.”

Therefore, it is appropriate to sanction the DGSEPE with a warning for the infringement

of article 32 of the GDPR,

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE the D.G. OF THE PUBLIC EMPLOYMENT SERVICE, with NIF

S7800001E, for a violation of Article 5.1.f) of the GDPR typified in Article

83.5 of the GDPR, a warning sanction.

IMPOSE the D.G. OF THE PUBLIC EMPLOYMENT SERVICE, with NIF S7800001E, for

an infringement of Article 32 of the GDPR typified in Article 83.4 of the GDPR, a

warning sanction.

SECOND: NOTIFY this resolution to D.G. OF THE PUBLIC SERVICE OF

EMPLOYMENT.

THIRD: COMMUNICATE this resolution to the Ombudsman, in

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

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 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 reversal before the

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

count 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 for in article 46.1 of the

referred Law.

Finally, it is noted 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 through

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

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

web/], or through any of the other registries 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 proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es