 File No.: EXP202101350

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. (hereinafter the claimant) on 07/07/2021 filed

claim before the Spanish Data Protection Agency. The claim is

directed against the STATE PUBLIC EMPLOYMENT SERVICE with NIF Q2819009H (in

forward the claimed). The grounds on which the claim is based are as follows:

that he has received a letter from the one claimed in which they appear printed in the

about (visible from the outside, therefore) personal data that should not be

expose yourself

And it provides a photograph of one of the sides of the envelope of the letter received. the letterhead

reference to the claimed party and includes the name, surname and address of the party

claimant. Likewise, it includes the following data: “Exp.: ***EXP.1”, “N.I.F./N.I.E.:

***NIF.1”

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), on 08/24/2021 said claim was transferred to the respondent

in accordance with the provisions of the LPACAP, to proceed with its analysis and

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

comply with the requirements set forth in the data protection regulations. Not included or provided

Respondent's response.

THIRD: On 10/28/2021, in accordance with article 65 of the LOPDGDD,

the claim filed by the claimant was admitted for processing.

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

of previous investigative actions to clarify the facts in

issue, having knowledge of the following extremes:

Dated 02/03/2022, it has a written entry from the claimed party indicating that it does not

There is no notification from the AEPD in relation to the facts investigated.

Causes of the incident and reaction measures

The inspection of services of the claimed party shows the following in relation to the

facts object of the claim that: “In the postal communications addressed by the

SEPE to applicants and/or beneficiaries of unemployment benefits

only the data necessary for delivery by the postal operator are visible,

that is, the name and surnames and the postal address of the interested party. In the month of June

In 2021, a change was made to the agency's communications templates.

As a result of this change, an incident occurred that caused the

moved the data, so a batch of erroneous communications was issued.

The incident was detected and corrected as quickly as possible, without

I have been aware of other complaints in this regard.”

FIFTH: On 04/26/2022, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

infringement of articles 5.1.f) and 32.1 of the RGPD, sanctioned in accordance with the

provided in article 83.5.a) and 83.4.a) of the aforementioned RGPD and considering that the

sanction that could correspond would be a WARNING. The reception consists

by the defendant of the agreement to initiate the file.

SIXTH: Once the initiation agreement has been notified, the one claimed at the time of this The resolution has not presented a written statement of allegations, for which reason the indicated in article 64 of Law 39/2015, of October 1, on the Procedure Common Administrative Law of Public Administrations, which in section f) establishes that in the event of not making allegations within the period established on the content of the initiation agreement, it may be considered a proposal for resolution when it contains a precise statement about the responsibility imputed, reason why a Resolution is issued.

SEVENTH: Of the actions carried out in this procedure, they have been accredited the following:

PROVEN FACTS

FIRST. On 07/07/2021 there is an entry in the AEPD written by the claimant stating that he has received a letter from the respondent appearing printed on the envelope (visible from the outside) personal data that should not be revealed.

SECOND. The claimant provides a photograph of one of the sides of the letter envelope received; include the reference letterhead of the respondent; name, surname and claimant's address. It also incorporates the following data: “Exp.: ***EXP.1”, “N.I.F./N.I.E.: ***NIF.1”.

THIRD. The respondent in writing dated 02/03/2022 has stated that “…In the month June 2021, a change was made to the communications templates of the organism. As a result of this change, an incident occurred that caused the data to shift, so a batch of wrong communications.

The incident was detected and corrected as quickly as possible, without

had evidence of other complaints in this regard”

FOUNDATIONS OF LAW

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, 48.1, 64.2 and 68.1 of the

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

Yo

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/10

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 Agency for Data Protection will be governed

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

regulatory provisions issued in its development and, insofar as they are not

contradict, in the alternative, by the general rules on the

administrative procedures.”

The claimed facts materialize in the sending by the claimed of a

letter whose envelope contains personal data that could violate the

regulations on the protection of personal data.

II

Article 5 of the RGPD establishes the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

The cited article 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 processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality”)”.

(…)

III

The documentation in the file offers clear indications that the

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

allow access to the personal data of the claimant, such as

consequence of the remission by the respondent of a letter whose envelope contains the

themselves.

This duty of confidentiality must be understood to have the purpose of

prevent access to data not consented to by the owners of the data.

themselves.

Therefore, this duty of confidentiality is an obligation that falls not

only to the person in charge and in charge of the treatment but to everyone who intervenes in

any phase of the treatment and complementary to the duty of professional secrecy.

Article 83.5 a) of the RGPD, considers that the infringement of “the principles

basic for the treatment, including the conditions for the consent in accordance with

of articles 5, 6, 7 and 9” is punishable.

IV

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

“Infringements considered very serious:

1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

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

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

(…)”

Second, article 32 of the RGPD “Security of treatment”,

v

establishes that:

"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 the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to 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.

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.

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 controller or the

manager and has access to personal data can only process said data

following the instructions of the person in charge, unless it is obliged to do so by virtue of the

Law of the Union or of the Member States".

The violation of article 32 of the RGPD is typified in the article

83.4.a) of the aforementioned RGPD in the following terms:

SAW

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

with 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.

(…)"

For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "Infringements considered serious":

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

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

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

following:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance

to what is required by article 32.1 of Regulation (EU) 2016/679".

(…)"

The facts revealed could imply the violation of the

technical and organizational measures violating the confidentiality of the data and

allowing access to them included in the envelope of the letter sent by the

Employment Service.

The GDPR defines personal data security breaches as

"all those violations of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

otherwise, or unauthorized communication or access to such data".

7th

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

that the claimed party has violated article 32 of the RGPD, when an incident of

security in your system allowing access to personal data of the claimant,

with the violation of technical and organizational measures.

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

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

object of treatment, but it 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

that the treatment entails, 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 measures

technical and organizational information must be carried out taking into account: pseudonymization and

encryption, the ability to ensure the confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (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
provided in 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 guarantee an adequate level of security, including
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.

In the present case, as evidenced by the facts and within the framework of the
investigation file the AEPD transferred the claimed on 08/24/2021 the
claim submitted for analysis requesting the provision of information
related to the incident claimed, without sending a response in this regard.

However, on 01/19/2022 a new request for information was sent and the
02/03/2022 sent a response indicating that there was no record of any notification of the
AEPD and that the claimed incident was due to the fact that "In the month of June 2021,

made a change to the agency's communications templates. What

As a result of this change, an incident occurred that caused the

moved the data, so a batch of erroneous communications was issued."

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

security revealed by the claimant, since it is responsible for taking

decisions aimed at effectively implementing technical measures and

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

to ensure the confidentiality of the data, restoring its availability and preventing

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

In accordance with the foregoing, it is estimated that the respondent would be

allegedly responsible for the infringement of the RGPD: the violation of article 32,

infraction typified in its article 83.4.a).

Notwithstanding the foregoing, also the LOPDGDD in its article 77, Regime

applicable to certain categories of controllers or processors,

sets the following:

viii

"1. The regime established in this article will be applicable to treatments

of which they are responsible or entrusted:

a) The constitutional bodies or those with constitutional relevance and the

institutions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

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

autonomous communities and the entities that make up the Local Administration.

d) Public bodies and public law entities linked or

dependent on the Public Administrations.

e) The independent administrative authorities.

f) The Bank of Spain.

g) Public law corporations when the purposes of the treatment

related to the exercise of powers of public law.

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Assemblies

Autonomous Legislative, as well as the political groups of the Corporations

Local.

2. When the managers or managers listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law, 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.

The resolution will be notified to the person in charge or in charge of the treatment, to the

body on which it reports hierarchically, where appropriate, and those affected who have

the condition of interested party, if any.

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

data protection will also propose the initiation of disciplinary actions

when there is sufficient evidence to do so. In this case, the procedure and

sanctions to apply will be those established in the legislation on disciplinary regime

or sanction that results from application.

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

and the existence of technical reports or recommendations for treatment is proven

that had not been duly attended to, in the resolution imposing the

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

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

correspond.

4. The data protection authority must be informed of the

resolutions that fall in relation to the measures and actions referred to

the previous sections.

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

analogous of the autonomous communities the actions carried out and the

resolutions issued under this article.

6. When the competent authority is the Spanish Agency for the Protection of

Data, it will publish on its website with due separation the resolutions

referred to the entities of section 1 of this article, with express indication of the

identity of the person in charge or in charge of the treatment that would have committed the

infringement.

When the competence corresponds to a regional protection authority

of data will be, in terms of the publicity of these resolutions, to what is available

its specific regulations.

According to the available evidence, the conduct of the

claimed constitutes the infringement of the provisions of articles 5.1.f) and 32.1 of the

GDPR.

It should be noted that the LOPDGDD contemplates in its article 77 the sanction of

warning in relation to the processing of personal data that is not

match your forecasts. In this regard, article 83.7 of the RGPD contemplates that

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

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

can, and to what extent, impose administrative fines on authorities and organizations

public authorities established in that Member State.

In this same sense, article 58 of the RGPD, in its section 2 d) indicates

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

treatment that the treatment operations comply with the provisions of the

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

specified period…".

As indicated previously, it has been proven that the defendant

has breached the data protection regulations, articles 5.1.f) and 32.1 of the RGPD, by

enable access to the personal data of the claimant, by sending the

claimed a letter in whose envelope the same appear, violating the measures

technical and organizational.

However, in its response to this directive center on 02/03/2022 the

claimed has indicated having corrected the incidence produced stating ".. In the

month of June 2021 a change was made in the communication templates

of the organism. As a result of this change, an incident occurred that

caused the data to shift, so a batch of

wrong communications.

The incident was detected and corrected as quickly as possible, without

has been aware of other complaints in this regard.

Therefore, it is considered that the response has been reasonable, having

corrected the incidence and not proceeding to urge the adoption of additional measures.

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 PUBLIC SERVICE OF STATE EMPLOYMENT, with NIF

Q2819009H, for an infringement of article 5.1.f) of the RGPD, typified in article

83.5.a) of the RGPD, a sanction of warning.

SECOND: IMPOSE the PUBLIC SERVICE OF STATE EMPLOYMENT, with NIF

Q2819009H, for an infringement of article 32 of the RGPD, typified in article

83.4.a) of the RGPD, a sanction of warning.

THIRD: NOTIFY this resolution to the PUBLIC EMPLOYMENT SERVICE

STATE.

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, the

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 period of month 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, the firm resolution may be provisionally suspended in administrative proceedings if the interested party expresses his intention to file a contentious appeal-administrative. If this is the case, the interested party must formally communicate this made by writing to the Spanish Agency for Data Protection, introducing him to the agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the filing of the contentious-administrative appeal within two months from the day following the notification of this resolution, it would end the precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es