 Procedure No.: PS/00203/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Ms. A.A.A. (hereinafter the claimant) on 08/07/2020 filed

claim before the Spanish Data Protection Agency. The claim is

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

hereinafter SEPE or claimed). The grounds on which the claim is based are

following: that when downloading a SEPE certificate you have accessed the data of

another person. Together with the claim, it provides evidence of what has been reported by means of

a screen dump containing the personal data of a third party.

SECOND: Upon receipt of the claim, the Subdirectorate General for

Data Inspection proceeded to carry out the following actions:

On 10/09/2020, the claim submitted was transferred to the defendant for analysis

and communication of the decision adopted in this regard. Likewise, he was required to

that within one month it send certain information to the Agency:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant.

The respondent answers this Agency, on 11/19/2020, indicating that it has been

The incident has been corrected and the claimant has been notified. does not credit the

manifested.

On 03/23/2021, the respondent is requested to provide a copy of the answer

provided to the claimant.

THIRD: On 04/29/2021, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed by the claimant against the respondent.

The respondent, on 05/11/2021, accompanies the letter sent to the claimant in the

indicating that there is no anomaly, after checking their certificates.

FIFTH: On 08/16/2021, 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 article 5.1.f) of the RGPD, sanctioned in accordance with the provisions of the

article 83.5.a) of the aforementioned RGPD and considering that the sanction that could

to correspond would be a WARNING.

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 08/07/2020 there is a written entry in the AEPD from the claimant

stating that by going to download a SEPE certificate you have accessed the data of

another person.

SECOND. The claimant provides a copy of her DNI nº ***NIF.1.

THIRD. The claimant provides a screen print of the electronic headquarters, office

virtual of the claimed in which the personal data of a third party is recorded when entering

the applicant's ID.

BEDROOM. There is a written document from the respondent sent to the claimant, dated 05/10/2020, in the

That points; “Once the pertinent verifications have been carried out, we have been able to

verify that the certificates requested by you and issued by the Public Service

of State Employment appear all in your name and with your data, not being able to observe

any anomaly.

Also, indicate that this response will be transferred to the Spanish Agency for

Data Protection".

It also provides the document sent to the AEPD informing in the sense indicated

previously.

FOUNDATIONS OF LAW

By virtue of the powers that article 58.2 of the RGPD recognizes to each

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

I

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

The facts denounced materialize in the access to data of third parties

violating the duty of confidentiality, on the occasion of the request for certificates

to SEPE.

II

Article 58 of the RGPD, Powers, states:

"two. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

b) send a warning to any person responsible or in charge of the treatment

when the treatment operations have infringed the provisions of the

this Regulation;

(…)”

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”.

III

The cited article states that:

"one. 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")".

(…)

On the other hand, article 5, Duty of confidentiality, of the new Law

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

digital rights (hereinafter LOPDGDD), states that:

"one. Those responsible and in charge of data processing, as well as all

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary

of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain

even when the relationship of the obligor with the person in charge or person in charge had ended

of the treatment".

IV

The documentation in the file offers clear indications that the

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

relation to article 5 of the LOPGDD, duty of confidentiality, by allowing the

access to the data of a third party when downloading a SEPE certificate.

This duty of confidentiality, previously the duty of secrecy, must

understood that its purpose is to prevent leaks of data not

consented to by their owners.

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.

v

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, it should be noted that the security of personal data

It is regulated in articles 32, 33 and 34 of the RGPD.

SAW

Article 32 of the RGPD "Security of treatment", establishes that:

"one. 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:

"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 in this claim materialize

in the breach of the technical and organizational measures violating the

confidentiality of the data allowing access to third party data when proceeding

to download the certificate from the Employment Service via the web.

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 third parties, with

violation of the established 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 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. Are

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.

In the present case, as evidenced by the facts and within the framework of the

investigation file E/07988/2020, the AEPD transferred the claimant the

claim submitted for analysis requesting the provision of information

related to the claimed incident. And although the claimant sent the AEPD the

response sent on 05/10/2020 to the respondent in which he indicated that once

carried out the pertinent checks, it was verified that the certificates

requested and issued were all in his name and with his personal data, not

there being any anomaly, it did not prove or justify at any time the

reality of the manifest.

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

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

typified in article 83.4.a).

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

Regime applicable to certain categories of persons responsible or in charge of

treatment, states the following:

viii

"one. 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 RGPD, without prejudice to the provisions of article 83,

contemplates in its article 77 the possibility of resorting to the sanction of warning

to correct the processing of personal data that is not in accordance with your

forecasts, when those responsible or in charge listed in section 1

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

this organic law.

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

allow access to the data of a third party when downloading a SEPE certificate, with

breach of technical and organizational measures.

It is necessary to point out that if these deficiencies are not corrected by adopting

the appropriate measures as indicated in articles 5.1.f) and 32.1 of the RGPD or

reiterate the behavior revealed in the claim and that is the cause of the

this procedure, as well as not immediately informing this AEPD of the

measures adopted could give rise to the exercise of possible actions before the

responsible for the treatment in order to apply effectively the measures

appropriate to guarantee and not compromise the confidentiality of the data of

personal character and the right to privacy of individuals.

However, it is true that in his response to this directive center the claimed

has indicated having corrected the claimed incidence, but it is no less so that it has not

accredited or justified the reality of said manifestations, not providing evidence

some of it; therefore, it is required that within a month provide the

measures adopted correcting the effects of the infraction produced.

Therefore, based on the foregoing,

By the Director of the Spanish Data Protection Agency,

HE REMEMBERS:

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

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

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

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

Q2819009H, for the infringement of article 32.1 of the RGPD, typified in article

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

THIRD: REQUEST the STATE PUBLIC EMPLOYMENT SERVICE, with NIF

Q2819009H, so that, within a month from the notification of this resolution,

accredits: the adoption of the pertinent measures adapting them to the regulations in

matter of personal data protection, correcting the effects of the

infraction produced, in accordance with the response offered to this body on

05/11/2020.

FOURTH: NOTIFY this RESOLUTION to the PUBLIC SERVICE OF

STATE EMPLOYMENT.

FIFTH: COMMUNICATE this resolution to the Ombudsman, 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 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

www.aepd.es

sedeagpd.gob.es