

□ Procedure No.: PS/00168/2021

## RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and with

based on the following

### BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) dated November 5, 2020

filed a claim with the Spanish Data Protection Agency. The

claim is directed against REGIONAL HEALTH MANAGEMENT OF CASTILLA AND

LEÓN with CIF S4711001J (hereinafter, the claimed). The reasons on which the

claim are:

□ Sending by the claimant via email to all applicants for

job offered the list of the 738 applicants in which the name,

surnames, telephone and email address, including those of the claimant.

SECOND: In view of the facts denounced in the claim and the

documents provided by the claimant / of the facts and documents of which he has

had knowledge of this Agency, it proceeds to initiate sanctioning procedure to the

claimed, in accordance with the grounds of law set forth below.

THIRD: On April 27, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, with

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), for the alleged violation of Article 32 of the RGPD, Article 5.1.f) of the

RGPD, typified in Article 83.4 of the RGPD.

FOURTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written

allegations in which, in summary, he accepted the terms of the initial agreement in all

its breadth and in which it exposes the technical and organizational means implemented to avoid repetition of events. It does not propose practice tests.

FIFTH: On 06/15/2021, a Resolution Proposal was issued in the following terms:

<<That the Director of the Spanish Data Protection Agency sanction REGIONAL HEALTH MANAGEMENT OF CASTILLA Y LEÓN, with CIF S4711001J, by the infringement of article 32 of the RGPD typified in Article 83.4.a) of the RGPD and by the infringement of article 5.1.f) of the RGPD typified in Article 83.5.a) of the RGPD, both with sanction of WARNING.

Likewise, it is considered that adequate measures have been taken to prevent recurrence of the personal data security incident referred to, so there is no the person responsible for the adoption of new measures is required.>>.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

2/6

SIXTH: After the deadline for submitting allegations to the Proposal for Resolution, they are not presented in this AEPD.

Of the actions carried out in this procedure and the documentation in the file, the following have been accredited:

#### PROVEN FACTS

FIRST: Of the documentation provided and the allegations made by the claimed, it is accredited that the claimed sent all applicants for employment offered the complete list of the 738 applicants in which the name, surnames, telephone and email address of all, including those of the claimant.

## FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016 on the protection of individuals with regard to the processing of personal data and the free circulation of these data and repealing Directive 95/46/CE (RGPD) recognizes each control authority, and according to the provisions of articles 47 and 48 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (LOPDGDD), the Director of the Spanish Agency for Data Protection is competent to initiate and resolve this procedure.

It should be noted that the documentation provided by the respondent shows that have implemented the appropriate technical and organizational measures to avoid repetition in the future of events similar to the one analyzed now.

II

III

Article 5.1.f) of the RGPD, Principles related to treatment, states the following:

"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 ("integrity and confidentiality").

Article 32 of the RGPD, the following:

IV

"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:

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

3/6

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 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.

Article 83.4 of the RGPD provides the following:

v

"4. Violations of the following provisions will be sanctioned, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or, in the case of a company, an amount equivalent to a maximum of 2% of the

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

the largest amount:

a) the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 a 39, 42 and 43;"

In the present case, there is a possible violation of articles 25 and 32 of the RGD, ,

Therefore, the provisions of art. 83.4 of the GDPR transcribed above.

Article 83.5 of the RGD provides the following:

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

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

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

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

the largest amount:

a)

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

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

Article 71 of the LOPDGDD provides the following.

<Constitute infractions 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.>

Article 72.1.a) of the LOPDGDD provides the following:

Violations considered very serious.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

<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 73.g) of the LOPDGDD provides the following:

<Infringements considered serious.

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:

g) The breach, as a consequence of the lack of due diligence, of the technical and organizational measures that have been implemented as required by article 32.1 of Regulation (EU) 2016/679.>

Article 77 of the LOPDGDD provides the following:

<Regime applicable to certain categories of persons responsible or in charge of treatment.

1. The regime established in this article will be applicable to the treatment of who are responsible or in charge:

a) The constitutional bodies or those with constitutional relevance and the institutions of autonomous communities analogous to them.

b) The jurisdictional bodies.

c) The General Administration of the State, the Administrations of the communities autonomous 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 purposes of the treatment are related to the exercise of legal powers public.

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Legislative Assemblies autonomous, as well as the political groups of the Local Corporations.

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

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

5/6

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 of the that depends hierarchically, where appropriate, and to those affected who had the condition interested party, if any.

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

sufficient evidence for it. In this case, the procedure and the sanctions to be applied will be those established in the legislation on disciplinary or sanctioning regime that result of application.

Likewise, when the infractions are attributable to authorities and managers, and proves the existence of technical reports or recommendations for the treatment 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 notified 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.

6. When the competent authority is the Spanish Data Protection Agency, this will publish on its website with due separation the resolutions referring 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 had committed the infraction.

When the competence corresponds to a regional authority for the protection of data will be, in terms of the publicity of these resolutions, to what your specific regulations.>

In the present case, from the documentation provided by the claimant and not refuted by the claimed, it is clear that the principle of integrity (security) has been violated as stated in article 32 of the RGPD, typified in article 83.4.a) of the RGPD and considered serious for prescription purposes in article 73.g) of the LOPDGDD, as well



as the principle of confidentiality as indicated in article 5.1.f) of the RGPD,  
typified in article 83.5.a) of the RGPD and considered very serious for the purposes of  
prescription in article 72.1.a) of the LOPDGDD.

In the present case, it is considered that adequate measures have been taken to  
prevent the aforementioned personal data security incident from occurring again,  
therefore, the person responsible for the adoption of new measures is not required.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

6/6

Therefore, in accordance with the applicable legislation and having assessed the criteria for  
graduation of the sanctions whose existence has been proven, the Director of the  
Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE THE REGIONAL HEALTH MANAGEMENT OF CASTILLA Y LEÓN,  
with CIF S4711001J, for the infringement of article 32 of the RGPD, typified in article  
83.4.a) of the RGPD the sanction of WARNING, and for the infringement of article  
5.1.f) of the RGPD,  
the sanction of  
WARNING.

typified in article 83.5.a) of the RGPD

SECOND: NOTIFY this resolution to the claimed and claimant.

THIRD

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-](https://sedeagpd.gob.es/sede-electronica-web/)

[web/](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

938-131120

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)