 File No.: PS/00442/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the complaining party) on 06/03/2021 filed

claim before the Spanish Data Protection Agency. The claim is

directs against NATIONAL AGENCY FOR ASSESSMENT OF QUALITY AND

ACCREDITATION with NIF S2801299E (hereinafter, ANECA). The reasons in which

the claim is based on are as follows:

-That, in accordance with the provisions of the Resolution of December 17, 2020

of the General Secretariat of Universities, submitted to ANECA a request for

evaluation of their research activity.

-That the result of the Resolution of the Plenary of the National Commission be communicated

Research Activity Evaluator (CNEAI), whose evaluation is negative, and

Attached as motivation for this resolution is the Report of the Advisory Committee, but, in

Instead of just giving you their report, they send you a 58-page document in

which, in addition to his, appear 28 more Reports.

Together with the claim, the claimant party did not provide any evidence or document

to justify your claim, so on 06/24/2021, the Director of the

Spanish Agency for Data Protection (hereinafter, AEPD) rejected the

claim.

SECOND: On 07/12/2021, the claimant filed an Appeal for

Replacement against the resolution of inadmissibility, contributing with the same various

reports issued by ANECA on behalf of different people, as well as a written

signed by the Head of the Quality Unit acknowledging the error made, and

It is communicated that they have proceeded to adopt the necessary measures to guarantee that

a similar incident will not occur again.

THIRD: On 08/18/2021, the Director of the AEPD estimates the Appeal for

Replacement, being notified to the complaining party on 08/30/2021

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

of previous investigative actions to clarify the facts in

question, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

BACKGROUND

This investigation is based on the claim filed on June 3,

2021 by A.A.A. (hereinafter, claimant party), being as claimed the AGENCY

NATIONAL QUALITY ASSESSMENT AND ACCREDITATION (hereinafter,

ANECA) and which gave rise to procedure E/07213/2021.

On April 4, 2022, within the framework of AI/00138/2022, it was decided to

information request to ANECA. In this requirement,

information marked by the following line of research:

- Know details about the notification of the security incident to all

affected.

information.

- Know the details about the aforementioned internal leak procedure

- Know the details about the existence of a documentary record of the incident.

-

Have more information about the possible permanence of the erroneous report in

the files of ANECA of the people affected.

On April 19, 2022, with registry entry REGAGE22e00013723923,

receives a response to this request, which is analyzed in the section “result of

investigative actions”.

INVESTIGATED ENTITIES

During these proceedings, the following entity has been investigated:

NATIONAL QUALITY ASSESSMENT AND ACCREDITATION AGENCY with NIF

S2801299E

RESULT OF THE INVESTIGATION ACTIONS

In relation to the response received from ANECA to the request for

information and that gave rise to the entry REGAGE22e00013723923, it is concluded:

- ANECA confirms that it did send notification of the incident to the different

affected dated June 8, 2021 through emails issued

from the cneai-comunicacion@aneca.es account. In this mail it was provided

the next information:

1. That during the notification process of six-year research periods of

the 2020 Call, several reports of the Advisory Committee of the field 09

were generated incorrectly by ANECA's computer application called

“CNEAI management application”, and instead of providing the information

of each request, in each report the information of other

negative requests from field 09, without any type of error.

2. That as soon as ANECA became aware of this fact, they contacted

implement all relevant technical and organizational measures to

solve it, following the steps marked by the PROCEDURE

INTERNAL INFORMATION LEAK in order to guarantee the

data protection regulations, analyzing whether there had been

security breach that must be notified to the AEPD and the

affected people, adopting additional measures to

ensure that a similar incident does not happen again.

- We are provided with the internal information leakage procedure, this

procedure is marked by a series of phases to be carried out to

manage a security incident, the content of

each of them:

(…)

- They confirm that ANECA followed the information leak procedure

previously summarized.

- In relation to the description of the facts, they provide us with:

1. That for the 2020 call for six-year terms CNEAI, a

series of developments for the web application with which it has been managed

Until now, this procedure, called "Management application

CNEAI". These developments mainly consist of integrating the

old six-year evaluation application with the ACCEDA system,

of the General Secretariat of Digital Administration (SGAD). For the

communication of the resolutions to the citizen, a

process that notifies several PDF files through the platform

ACCESS, one of these files with the result of the assessment. The

generation of this document as such SI is a new development. In

In case the resolution is negative, another

file with the report of the committee, containing the observations of

each contribution, the generation of this document is NOT a new

developing. The generation of these files should be unique for each

request, and tests were performed in a pre-production environment without

find strange behavior.

2. That on June 2 they carried out a test with few files in

the production environment and verified that everything was correct.

3. That on the same day, June 2, they launched the process to notify the

field resolutions 09.

4. That for said field there were 26 negative resolutions out of 26

people and that the code that generated the committee report was executed

for each request (this code was not part of the new development).

5. That the same day, June 2, they receive an email from a

of people notified indicating the error in the PDF file

received. Verifying by ANECA the error in the generation of the

file for field 09, stopping the process immediately

for the rest of the fields.

6. That the generated file contained 29 reports that corresponded to 26

files and 26 affected.

7. That they looked for an alternative way to generate correctly and

individualized the reports, proceeding to their correct notification in

around 12:53 p.m. the same day. It is confirmed to us that ANECA

solved the incident on the same day and that the

technical measures to prevent it from happening again.

8. That in ACCEDA the erroneous reports were eliminated and the

correct, however, they indicate that in ACCEDA the

first erroneous notifications made with the erroneous file

attached to each notification, that ANECA does not have the appropriate roles

in ACCESS to delete this information and that it was requested with, date

June 4, 2021, to ACCESS technical support for removal.

9. That the COMUNICA-BRECHA tool of this Agency was used

to assess the obligation to inform affected persons,

taking into account the following information:

 That the filtered data is identifying data (name,

surnames and NIF) as well as data on their professional situation.

 That the gap is detected on June 2, 2021.

 That the number of people affected is small and that

there had been a similar incident.

10. They indicate that they accept the mistake made, but that they trust the 26

affected recipients in the sense that they will not misuse the

information received, which means that the consequences of the failure are not

are serious when the probability of risk is eliminated. Secondly,

indicate that the impact for the people affected is not high, with

inconveniences that are easy to overcome, such as the discomfort generated,

reason why they conclude that there is no high risk for the rights and

freedoms of those affected.

11. They tell us that it is not appropriate to notify the notification of the breach before the

AEPD because they understand that it is unlikely that the gap constitutes a

risk to the rights and freedoms of the people affected. Of the

In the same way, they justify that it is not necessary to notify the breach to the

affected people.

12. However, for the sake of transparency, they indicate that ANECA sent

email to those affected explaining what happened, informing the

solution of the incidence and urging them to please eliminate the

reports received in error.

13. They indicate that ANECA's DPD has proceeded to

document the incident in the ANECA Breaches Registry, we

they provide a copy of this record and it is verified that it actually appears

this information.

14. They indicate that, as the main improvement measure, it is determined that

you should expand the test data set to cover a larger

range of possibilities and casuistries to test, before its execution

real.

15. That in relation to the erroneous notifications that continue to be

accessible in ACCEDA, on August 12, 2021 they received

response from the SGAD indicating that ACCEDA does not provide the

service to eliminate the procedures, files and documents, for

what in the notifications/communications section will continue to appear

next to the notification made.

CONCLUSIONS

- ANECA assumes the error that gave rise to the claim, confirming that

It was caused by failures in the application module that generated the files, after

having previously uploaded new versions of other application modules

to production, and having passed a series of tests previously. What

measure of improvement assume that the range of casuistries of

tests to be carried out prior to production start-up, so

deduces that the tests carried out were not exhaustive.

- No notification is made to the AEPD as it is considered unlikely that

there is a risk to the rights and freedoms of the people affected. Of the

In the same way, they indicate that it is not appropriate to notify the affected people,

However, they send mail to each affected with information on what happened and the

solution given, this shipment was made on June 8, 2021.

The erroneous files remain in ACCESS. ANECA contacted SGAD

to proceed with its elimination, but they answered that the platform does not provide the

service to delete the documents so in the section “notifications

done” continue to appear.

-

FOURTH: On May 19, 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 Article 5.1.f) of the RGPD and Article 32 of the RGPD,

typified in Article 83.5 of the RGPD.

Once notified of the initiation agreement, ANECA submitted a pleadings brief in which, in

synthesis stated:

-That ANECA applied the technical measures it considered pertinent and appropriate to the

risk, thus complying with article 32 of the RGPD. Accordingly, before

to proceed with the sending of notifications with the evaluation reports, had been

tested in a pre-production environment without finding behaviors

strangers. That, among the technical measures taken, a prior check was made to

guarantee the security of the data and the proper functioning of the new headquarters

electronic and of the new evaluation application were six-year terms, not finding

any abnormal operation.

In this regard, this Agency considers that the measures taken by ANECA

were not appropriate to guarantee an adequate level of security at

risk, as established in article 32 of the RGPD, since, in

In fact, it has been established that the negative reports in the

field 09 of the CNEAI management application, were not generated automatically.

individually for each applicant, giving rise to the incident substantiated in the

present sanctioning procedure.

-That always keeping in mind to guarantee adequate security in the treatment of

data, as prescribed in article 5.1.f) of the RGPD, and evaluating the adequacy of the

technical and organizational measures to be taken to guarantee a level appropriate to the risk

of data assurance, as prescribed in article 32.1 of the RGPD, it was decided

make a first notification of results in a field with few evaluations

negative, specifically, field 09, of the total of 14 existing scientific fields, and

that was when a failure occurred in the computer application, not detected

previously, and the 26 files were sent to the 26 people affected, a fact that

regrets, as was communicated to said persons.

In this regard, this Agency refers to what has already been stated in relation to the

previous allegation, in the sense of emphasizing that the measures were not

adequate. It is also worth mentioning recital 28 of the RGPD, according to which:

“The application of pseudonymization to personal data can

reduce risks to affected stakeholders and help stakeholders

responsible and those in charge of the treatment to comply with their

data protection obligations.

-That ANECA considers that it complied with the provisions of article 33.1 of the RGDP, in the

extent to which he made an assessment of what happened and considered it to be

unlikely that the security breach that had taken place constituted a risk

for the rights and freedoms of the natural persons affected, which is why it does not

notification was made to the AEPD, in accordance with the provisions of said

precept.

To carry out this evaluation, follow the steps that appear in your procedure.

internal, which include the recommendations that the AEPD itself has been giving, which

states that “Notifying all personal data breaches is not mandatory, given

that the RGPD provides for an exception to this obligation when, in accordance with the principle of

proactive responsibility, the controller can ensure that it is unlikely that the

breach of personal data entails a risk to the rights and freedoms of individuals

Physical persons".

In this regard, and taking into account that in this Procedure

Penalty has not been imputed infringement for breach of article 33

of the RGPD, this agency has nothing to add.

-That upon concluding that it was not likely that the security breach produced

would constitute a “HIGH” risk for the rights and freedoms of natural persons

affected, nor did they have to take any action to protect themselves or minimize

the consequences derived from the actions of this Organism, was why it was

affirms that it was not appropriate to carry out notification to them, as established by the

article 34 of the RGPD. And, nevertheless, ANECA wanted to be transparent, give

explanations and apologize, and, even considering that she was not involved in

the obligation to make the notification of a breach of personal data to the

affected people, he preferred to inform all of them about what happened and express his

upset about what happened.

In this regard, and taking into account that in this Procedure

Penalty has not been imputed infringement for breach of article 34

of the RGPD, this agency has nothing to add.

That the existence of mitigating elements must be taken into account, such as the

short duration of the breach, how quickly issues were detected and remediated

facts, the small number of people affected and the level of damages

suffered, as well as the categories of personal data that were seen

affected, which were in no case sensitive data, taking into account the

group in question. It also states that there was no intention to

part of ANECA, which took the precise measures that were considered pertinent to

mitigate possible damage, also complying with the steps established by the

regulations regarding how to act in the event of a possible breach of personal data.

Likewise, it indicates that there have been no more cases and the application “Gestión de CNEAI”

works properly, no other leaks or leaks have been known to exist.

data protection claim.

In this regard, this Agency points out that, when setting the sanction

corresponding to the infractions imputed in a procedure

Sanctioning, all factors are always taken into consideration

concurrent.

FIFTH: On June 30, 2022, a resolution proposal was formulated,

proposing:

That the Director of the Spanish Agency for Data Protection imposes

NATIONAL QUALITY ASSESSMENT AND ACCREDITATION AGENCY, with

NIF S2801299E, for an infringement of Article 5.1.f) of the RGPD, typified in the

article 83.5 of the RGPD, a sanction of warning.

That the Director of the Spanish Agency for Data Protection imposes

NATIONAL QUALITY ASSESSMENT AND ACCREDITATION AGENCY, with

NIF S2801299E, for an infringement of Article 32 of the RGPD, typified in Article

83.4 of the RGPD a sanction of warning.

SIXTH: Once the proposed resolution has been notified, ANECA presents a new written

allegations dated 07/20/2022, in which it mainly reiterates those already presented

to the Initiation Agreement and add that:

-They did not consider the application viable, in this evaluation procedure

of six-year terms, of measures such as the pseudonymization of personal data, taking into account

not only to the context and purpose of the treatment but also to the technical means with

those available in that Agency.

-It should also be noted that article 32 of the RGPD also states that among the

measures to apply for data security is the ability to

quickly restore the availability and access to personal data in the event

physical or technical incident, which has been shown to have occurred in this case,

where just in a few hours the technical incident that occurred was solved.

-In addition to the above, when evaluating the level of security and the measures taken to avoid

risks in the computer developments practiced that have been mentioned, it is

important to pay attention to the fact that it is a non-vulnerable group on which the

Twenty-first additional provision of Organic Law 4/2007, of April 12, by

which modifies Organic Law 6/2001, of December 21, on Universities,

establishes that the consent of university staff will not be required

for the publication of the results of the evaluation processes of its activity

teaching, research and management carried out by the university or by the agencies or

public evaluation institutions.

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 claimant submitted an application to ANECA

evaluation of their research activity.

SECOND: It is proven that when communicating to the complaining party the result of

the Resolution of the Plenary Session of the National Activity Evaluation Commission

Researcher (CNEAI), whose assessment was negative, was attached as motivation for

this resolution the Report of the Advisory Committee, a 58-page document in which,

In addition to its own report, there are 28 more corresponding to different

people.

THIRD: It is proven that during the notification process of six-year terms of

Call 2020 research, various Field Advisory Committee reports

09, (negative resolutions), were generated incorrectly by the ANECA computer application

called "CNEAI management application", and instead of providing the information of

each request, information from other negative requests was included in each report

from field 09.

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."

In relation to the arguments presented to the resolution proposal, ANECA substantially repeats those already presented in the initiation agreement, adding that:

II

1-This Body has not considered that the application would be viable, in this six-year evaluation procedure, of measures such as the pseudonymization of personal data, taking into account not only the context and purpose of the treatment, but in addition to the technical means with which they are available in this Organism.

But it should also be noted that article 32 of the RGPD also states that among the measures to apply for data security is the ability to

quickly restore the availability and access to personal data in the event physical or technical incident, which has been shown to have occurred in this case, where just in a few hours the technical incident that occurred was solved.

-In this regard, this agency considers that, even when the incident resolved quickly, the sending of reports of negative results had already been carried out, therefore, even when measures have subsequently been taken that may be more efficient, at the time of the incident the established measures were insufficient, in accordance with what is established Article 32 of the GDPR.

Likewise, it is indicated that the pseudonymization of data is an example of a measure

tending to avoid exposure of personal data, which, effectively, each

responsible or in charge of data must assess for its implementation, not

intending this agency to consider it tax, but a mere indication, and

not basing the breach of article 32 RGPD on its absence, but on the

verification of the insufficiency of all the measures adopted.

2-When evaluating the level of security and the measures taken to avoid risks in the

computer developments practiced that have been mentioned, it is important to attend to

that it is a non-vulnerable group on which the Additional Provision

twenty-first of Organic Law 4/2007, of April 12, which modifies the

Organic Law 6/2001, of December 21, on Universities, establishes that it will not be

The consent of the personnel of the universities is required for the publication of the

results of the evaluation processes of their teaching, research and

management carried out by the university or by public agencies or institutions of

evaluation.

-In this regard, this agency points out that, although the aforementioned provision

“Even so, it will not be necessary

additional, in its point 4 it establishes:

consent of the university personnel for the publication of the

results of the evaluation processes of their teaching activity,

research and management carried out by the university or by the agencies or

public evaluation institutions”, it cannot be applied to the present case, given

that the publication of the RESULT of the activity of the

claimant party and other teachers, but what has been sent by

email to each of them is the FULL REPORT, with all

the data, and not only the result, positive or negative, of the same, both

own as well as the rest of those evaluated negatively, so it cannot

take this provision into account.

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

III

"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 stated that the personal data of those affected, contained in the

ANECA database, were unduly exposed to a third party, since the

complaining party has provided to the file a copy of reports issued in the name of

other people, which he received along with his own.

From the investigation carried out in this proceeding, it is concluded that ANECA

has violated the provisions of article 5.1.f) of the RGPD, by sending jointly to

each of the applicants the reports of 26 people in which the data is recorded

personal to each of them.

Article 83.5 of the RGPD, under the heading "General conditions for the imposition

of administrative fines” provides:

IV

“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 largest 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 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 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 83 section 7 of the RGPD provides the following:

v

“7. 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.

For its part, 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 Local Administration.

(…)

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. (…)”

Article 32 “Security of treatment” of the RGPD establishes:

SAW

"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 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.

In the present case, at the time of the breach, ANECA was using a computer application for the generation of reports that, instead of generating a report for each individual request, generated information at the same time corresponding to other requests, revealing, therefore, data of various applicants to each of them, since each applicant received, at the same time as his own report, the one corresponding to the rest of the applicants.

Article 83.4 of the RGPD, under the heading "General conditions for the imposition of administrative fines", provides:

7th

"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 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.

(…)

Article 83 section 7 of the RGPD provides the following:

“7. 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.

For its part, 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 Local Administration.

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. (…)"

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:

IX

FIRST: IMPOSE the NATIONAL QUALITY ASSESSMENT AGENCY AND

ACCREDITATION, with NIF S2801299E, for a violation of Article 5.1.f) of the RGPD,

typified in Article 83.5 of the RGPD, a sanction of warning.

IMPOSE the NATIONAL QUALITY ASSESSMENT AGENCY AND

ACCREDITATION, with NIF S2801299E, for a violation of Article 32 of the RGPD,

typified in Article 83.4 of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to the NATIONAL AGENCY OF

QUALITY ASSESSMENT AND ACCREDITATION.

THIRD: 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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