File No.: PS/00059/2022

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On March 18, 2021, the Subdirectorate General for Inspection of

Data (SGID) received for its assessment a document of notification of breach of

security of personal data sent by the MINISTRY OF EDUCATION AND

CULTURA with NIF S3011001I (hereinafter, CEC), received on 03/06/2021, in the

that informs the Spanish Data Protection Agency of the following:

"(...)".

On 03/29/2021 a complementary notification is received with which it is provided,

as attached documentation, complaint filed with the General Directorate of the

Police, and a report prepared by the Subdirectorate General for Corporate IT

of the Ministry of the Presidency and Finance of the Region of ***LOCALIDAD.1, in the

that the scope, actions and damages are evaluated in relation to the security incident

produced.

SECOND: On 03/07/2021 a claim is received from A.A.A.. The reasons

on which the claim is based are as follows:

"(...)".

On 03/25/2021, in accordance with article 65 of the LOPDGDD, the

processing the claim and joins the file initiated after the notification of the breach

of security.

THIRD: On 03/12/2021 another claim is received from the (...), represented

by BBB Collegiate lawyer No. XXXX, of the Illustrious Bar Association of

*** LOCATION.1, in which the following is stated:

"(...)".

On 04/08/2021, in accordance with article 65 of the LOPDGDD, the

processing the claim and joins the file initiated after the notification of the breach

of security.

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

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 57.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the

following ends:

- On March 7, 2021, the IT services of the Community

Autonomous Region of ***LOCALIDAD.1 issued a statement announcing that

had suffered massive attacks on the systems of the MINISTRY OF EDUCATION

AND CULTURE. However, it was not made clear whether the attacks had been successful, and whether any

personal information had been exposed to strangers. The only action requested

since such services has been the change of password, up to four times in an end

of the week, with the consequent blocking of the accounts and the activity of its users.

- On the platform that has been the victim of the attack, data from some

37,500 teachers. Some of them have noticed that their bank details have been

modified. It is conjectured that the integrity or

confidentiality of other types of personal information that are also stored

on the platform, such as academic records, qualifications, teaching experience or

opposition notes.

Number of affected according to notification: XX.XXX.

Typology of data according to notification: username and password

They indicate that they have communicated the breach to those affected.

Regarding the company

The notifying entity is a Spanish public institution. It has been found in

files of the AEPD files prior to the present in relation to breaches of

this entity (E/04753/2020).

Information and documentation has been requested from the notifying entity, and from the

The response received shows the following:

Regarding the chronology of events. Actions taken in order to minimize

adverse effects and measures adopted for their final resolution

(...).

According to the documentation received (and which could not be verified), the measures

adopted to resolve the gap are satisfactory.

Regarding the causes that made the gap possible

(...).

It can be concluded from the documentation received that the measures have not been applied.

technical and organizational measures necessary to prevent the breach from occurring.

Regarding the affected data

(...).

Regarding the treatment manager contract

(...).

Regarding the security measures implemented

(...).

These supposed security measures previously implemented have not been able to

be verified, by not providing the claimed, proof of having implemented them.

It is doubted that there has been an effective access control, otherwise the breach will not be

would have produced since they indicate that it was produced by (...). Furthermore, they indicate that there

implemented different levels of access to data, a statement that remains in

questioned when in the section on “how the breach occurred” it is indicated:

“(…)”

Technical and organizational measures adopted to avoid, as far as possible, incidents such as

the happened.

(...).

- Other measures:

(...).

These measures could not be verified, but in themselves they seem sufficient to

avoid similar events in the future.

Information on the recurrence of these events and the number of similar events

events in time

(...).

FIFTH: On March 4, 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 32 of the RGPD, typified in Article 83.4 of the

GDPR.

Once the initial agreement was notified, the CEC presented a pleadings brief in which, in

summary, stated that:

-Although at first, it was considered that the incident was due to (...), and that

Article 32 of the RGPD is not considered infringed since, prior to the incident

that causes the data security breach, the Responsible had adopted

a series of technical and organizational measures aimed at data protection

of a personal nature and the security of information systems, therefore the origin

of the incident is not due to a lack of security measures, (...).

In this regard, it should be noted that, although the person responsible in his allegations

claims to have, prior to the breach, some certifications that

would accredit the implemented measures, it does not provide any documentary support that

accredit.

From the documentation in the file, it is inferred that the incident could be

have avoided with a double authentication system, and that the measures implemented

previously they were not adequate and sufficient to avoid it.

-Article 34 of the RGPD is not considered infringed, since the Responsible acted

diligently and proactively when informing the interested parties as a first measure of

reaction to the incident, and this taking into account, moreover, that it has not existed in

at no time a high risk for those affected that should launch the

communication to the interested parties in accordance with article 34 RGPD.

They also allege that to calculate the risk of the breach, the

methodology and guidelines of the AEPD. The risk is the result of multiplying the

chance impact. Due to the urgency of the situation, the

abbreviated procedure, the result of which is a low impact (severity of the breach) and

a medium chance. The factors taken into account to calculate the probability

have been: (A) the volume of affected (XX.XXX users), (B) the probability of

identify those affected (illegible data) and (C) the data affected in a period of

time (from November 2020). Consequently, transferring said data to the

matrix of Annex III of the incident management procedure, the risk of the breach

It is low.

In this regard, this Agency proceeds to analyze again the communications

made to those affected at the time of the breach, concluding that

it cannot be affirmed that article 34 of the RGPD has been breached, since the CEC

certifies not only having informed each of the affected teachers, but also

that the news was published in the press: ***URL.1.

Therefore, the allegations regarding the infringement of article 34 of the RGPD are considered.

refers, leaving without effect the initial imputation for non-compliance with said article.

SIXTH: On May 17, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

impose on the MINISTRY OF EDUCATION AND CULTURE, with NIF S3011001I, for a

infringement of Article 32 of the RGPD, typified in Article 83.4 of the RGPD a

warning sanction.

Once the aforementioned proposal was notified on 05/20/2022, there is no evidence that

filed arguments against it.

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 proven that on 03/04/2020, the CEC suffered an incident of

security, qualified as a breach of confidentiality, integrity and availability, by

having verified that the personal data of those affected have been

exposed to unauthorized third parties, that access passwords were changed, so

that some of those affected temporarily did not have access to their accounts, as well

like that bank details of some people were modified.

SECOND: It is proven that the CEC had a series of measures that did not

were neither appropriate nor sufficient, and that, according to its own initial statement at

respond to the request of the AEPD, the process of implementing the measures

derived from the risk analysis carried out at the time was not finalized at the

incident date.

THIRD: It is proven that the CEC communicated to those affected the incident of

security by sending an SMS, and that the IT services of the Region

from ***LOCALIDAD.1 sent an email to all teachers

informing them of what happened. In addition, the incident was reported to the unions and

published in the newspaper “***PERIÓDICO.1” of ***LOCALIDAD.1.

FOUNDATIONS OF LAW

Yo

Competition

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.”

II

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

Article 32 of the GDPR

"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.

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

At the time of the breach, the CEC did not have adequate measures

to prevent the occurrence of an incident such as the one under consideration in this

file, since as the CEC itself states, the origin of the gap is

because the process of implementing the measures derived from the analysis of

risks carried out at the time was not finalized at the date of the incident.

Classification of the infringement of article 32 of the RGPD

III

The infringement is typified in article 83.4 of the RGPD, which under the heading "Conditions

rules for the imposition of administrative fines" provides:

"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.

(…)

Sanction for the infringement of article 32 of the RGPD

IV

Article 83 section 7 of the RGPD, provides the following:

Without prejudice to the corrective powers of the control authorities under

of 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.”

Likewise, 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:

FIRST: IMPOSE THE MINISTRY OF EDUCATION AND CULTURE, with NIF

S3011001I, for an infringement of Article 32 of the RGPD, typified in Article 83.4

of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to the MINISTRY OF EDUCATION AND

CULTURE.

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.

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

938-050522

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es