 Procedure No.: PS/00176/2021

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 claimant) dated November 9, 2020

filed a claim with the Spanish Data Protection Agency (hereinafter

AEPD). The claim is directed against CLUB DEPORTIVO AKEKI DE TENERIFE

with NIF G76613041 (hereinafter, the claimed). The reasons on which the

claim are the publication, on the web page of the claimed and of public access,

of the DNI number, name, surnames, net salary and withholdings made from the

claimant. Together with the claim, it provides screenshots where the

publication of the aforementioned data.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the respondent, so that

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

On 01/04/2021, a response was received from the respondent. Based on the information

available, there are reasonable indications of a possible

violation of the regulations on data protection, without prejudice to what

determined in the course of the instruction of this procedure.

THIRD: On 04/15/2020, in accordance with the provisions of article 65 of the

LOPDGDD, the Director of the Spanish Data Protection Agency agreed to admit

processing the claim filed by the claimant against the respondent.

FOURTH: On June 28, 2021, the Director of the Spanish Agency for

Data Protection agrees to initiate sanctioning procedure to the claimed, for the

alleged infringement of article 5.1 f) of the RGPD, in accordance with the provisions of article

83.5 of the RGPD, considered very serious prescription effects in article 72

section 1. i) of the LOPDGDD, and for the alleged infringement 32 of the RGPD, in accordance with

the provisions of article 83.4 of the aforementioned RGPD, classified as serious for the purposes of

prescription in article 73 section f) of the LOPDGDD

FIFTH: Having notified the aforementioned initiation agreement and not having presented arguments,

in accordance with the provisions of article 64.2.f) of Law 39/2015, of October 1, of the

Common Administrative Procedure of the Public Administrations, the agreement of

start can be considered motion for a resolution. Consequently, this Agency

proceeds to dictate Resolution.

FACTS

FIRST: On November 9, 2020, the claimant filed a claim

before the Spanish Data Protection Agency, against the AKEKI SPORTS CLUB

DE TENERIFE with NIF G76613041 for the publication, on the website of the

claimed and of public access, of the DNI number, name, surnames, net salary and

withholdings made by the claimant

SECOND: On January 4, 2021, a response is received to the transfer of the

claim, of the documentation provided, the respondent states that he published in the

web page the external audit report to comply with the Transparency Law

of the Government of the Canary Islands, where they were visible, the DNI, the name and the amount of the

claimant's payroll. And that after receiving the claimant's request, he agreed to the

crossed out of the ID.

FOUNDATIONS OF LAW

Yo

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

control, 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

resolve this procedure.

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

II

"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 5 of the LOPDGDD, Duty of confidentiality, states the following:

"1. 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 to the

duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even when

the relationship between the obligor and the person in charge or in charge of the transaction had ended.

treatment".

The documentation in the file shows that the defendant violated the

article 5 of the RGPD, principles relating to treatment, in conjunction with article 5 of

the LOPGDD, duty of confidentiality, when publishing on its website, the DNI, the name and the

monthly payroll amount.

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

leaks of the data are carried out, not consented by the owners of these.

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

responsible 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

III

Regarding the security of personal data, article 32 of the RGPD "Security

of the treatment", establishes that:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular 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.

The facts revealed imply the violation of the measures

technical and organizational by making it possible to display the claimant's documentation

where your personal data is recorded with the consequent lack of diligence

by the person in charge.

IV

The GDPR defines personal data security breaches as “all

those breaches 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”.

From the documentation in the file, it is confirmed that the respondent has

violated article 32 of the RGPD, when a security incident occurred due to the

publication on its website of personal data of the claimant, allowing the

unauthorized access to these by third parties.

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

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

of treatment, but establishes that the person in charge and the person in charge of the treatment

apply technical and organizational measures that are appropriate to the risk involved

the treatment, taking into account the state of the art, the application costs, 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 technical measures and

organizational must be carried out taking into account: pseudonymization and encryption,

capacity to guarantee confidentiality, integrity, availability and resilience, the

ability to restore availability and access to data after an incident, process

verification (not audit), evaluation and assessment of the effectiveness of the

measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

"(83) In order to maintain security and prevent the treatment from violating the

provided in this Regulation, the person in charge or the person in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as

encryption. These measures must guarantee an adequate level of security, including

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

In this case, as evidenced by the facts and in the case file

E/09861/2020, the AEPD transferred to the defendant, the claim submitted for

analysis, requesting the provision of information related to the incident. Of the documentation provided, the respondent states that he published on the website the external audit report to comply with the Transparency Law of the Government of Canary Islands, where they were visible, the DNI, the name and the amount of the payroll of the claimant. And that after receiving the claimant's request, he agreed to cross out the DNI.

However, the regulatory bases of the subsidy contained in the Order of 10 December 2019, published in the BOC on 12/19/2019, in its article 16 establishes the obligations of the beneficiary.

Specifically in the two. 4. “Compliance, at all times, with the provisions of the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of the digital rights (BOE nº 294, of 12.6.18)”.

Likewise, point three of the aforementioned article provides, “in compliance with article 3.1, letter b) in relation to article 13 of Law 12/2014, of December 26, of transparency and access to public information, publicity must be made of the subsidies obtained, derived from this call, and specifically in section a) reference is made to the case in which the website of the beneficiary person, establishing that it should be added to the menu, on the page major,. an icon under the name of grants, which will be inserted in pdf format, the final resolution (granting the subsidy)”.

Therefore, and in accordance with the aforementioned regulations, only the resolution granting the subsidy, lacking a legitimating basis, for the publication of the personal data contained in the external audit report.

The liability of the claimed party is determined by the security breach revealed by the claimant, since he is responsible for making decisions aimed at effectively implementing the technical and organizational measures appropriate to guarantee a level of security appropriate to the risk to ensure the

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

in the event of a physical or technical incident.

In accordance with the foregoing, the respondent is responsible for the violation of the

article 32 of the RGPD, infringement typified in article 83.4.a) of the RGPD.

From the actions carried out, it is confirmed that the security measures, both

technical and organizational nature, with which the investigated entity had in

relation to the data that it submitted to treatment, were not adequate at the time

if the security breach occurs.

The consequence of this lack of adequate security measures was the exposure

to third parties unrelated to the personal data of the workers of the investigated company. It is

In other words, those affected have been deprived of control over their personal data.

This risk must be taken into account by the data controller who, in

function of this, must establish the necessary technical and organizational measures that

prevents the data controller from losing control of the data and,

therefore, by the owners of the data that provided them. The

violation of the principle of confidentiality (art 5.1.f) RGPD), the absence of measures

of security (art 32 RGPD) adequate according to the risk, constitute the element

of guilt that requires the imposition of a sanction.

v

In the present case, there is a violation of article 5.1.f) of the RGPD, so it is

application of the provisions of art. 83.5 of the GDPR.

Article 83.5 of the RGPD 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)

basic principles for treatment, including conditions for con-

sentiment under articles 5, 6, 7 and 9;"

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what

following: Violations constitute the acts and conducts referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

Establishes article 72 of the LOPDGDD, under the rubric of infractions considered

very serious, the following: "1. Based on the provisions of article 83.5 of the

Regulation (EU) 2016/679 are considered very serious and will expire after three years

infractions that suppose a substantial violation of the articles

mentioned therein and, in particular, the following:

(…)

Yo)

The violation of the duty of confidentiality established in article 5 of

this organic law.

The violation of article 32 RGPD is typified in article 83.4.a) of the

cited RGPD in the following terms:

"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 the person in charge in accordance with articles 8, 11,

25 to 39, 42 and 43."

(…)

It establishes article 73 of the LOPDGDD, under the heading "Infringements considered

serious", the following:

"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 result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679.

In the present case, the infringing circumstances provided for in article

83.5 and 83.4 of the RGPD and 72.1 i) and 73 section f) of the LOPDGDD, transcribed above.

SAW

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III on the "Principles of the power to impose penalties", in article 28

under the heading “Responsibility”, the following:

"1. They may only be sanctioned for acts constituting an administrative infraction.

natural and legal persons, as well as, when a Law recognizes their capacity to

to act, the affected groups, the unions and entities without legal personality and the

independent or autonomous estates, which are responsible for them

title of fraud or guilt.”

Article 58.2 of the RGPD, states the following:

7th

2. Each supervisory authority will have all of the following corrective powers

listed below:

(...) "

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

when the treatment operations have infringed the provisions of the

this Regulation.”

Establishes article 76 of the LOPDGDD under the heading "Sanctions and measures

corrective measures”, the following: “1. The penalties provided for in sections 4, 5 and 6

of article 83 of Regulation (EU) 2016/679 will be applied taking into account

the graduation criteria established in section 2 of the aforementioned article.

(…)

3. It will be possible, complementary or alternatively, the adoption, when

appropriate, of the remaining corrective measures referred to in article

83.2 of Regulation (EU) 2016/679."

viii

Article 70.1 of the LOPDGDD indicates the responsible subjects.

"1. They are subject to the sanctioning regime established in the Regulation (EU)

2016/679 and in this organic law:

a) Those responsible for the treatments."

In the present case, based on the diligence carried out by the entity

investigated in relation to proceeding to cross out the DNI of its employees, as well as

as well as the response to the request made by the AEPD, justifying its action

in compliance with the Transparency Law of the Government of the Canary Islands, allows

consider a decrease in guilt in the facts, so it is considered

in accordance with the law, not to impose a sanction consisting of an administrative fine and

replace it with the penalty of warning, in accordance with article 76.3 of the

LOPDGDD in relation to article 58.2 b) of the RGPD.

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 CLUB DEPORTIVO AKEKI DE TENERIFE, with NIF

G76613041, for violation of Article 32 of the RGPD, typified in Article 83.4 of the

RGPD and Article 5.1.f) of the RGPD, typified in Article 83.5 of the RGPD, a

warning sanction.

SECOND: NOTIFY this resolution to CLUB DEPORTIVO AKEKI DE

TENERIFE.

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es