 Procedure No.: PS/00044/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On October 6, 2020, D. A.A.A. (hereinafter, the claimant)

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the CLUB NAUTICO EL ESTACIO, with CIF G73044893 (in

later, the claimed one). The grounds on which the claim is based are: that this

entity has published on its website, the call and the Minutes of the Ordinary Meeting of the

Club, dated *** DATE.1, exposing your personal data, without restrictions of

access.

It has been verified that both documents are accessible on the website of the

reported entity.

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 December 17, 2020, a response was received from the respondent in which, in

synthesis, shows that it was placed on the bulletin board and on the website

as has always been the case, that only the members

of the Board of Directors and no member of the existing ones, that the Yacht Club of "El

Estacio" is located at ***ADDRESS.1, with only one store

meetings and hardly any sports functions and activities.

THIRD: On February 1, 2021, in accordance with 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: In view of the facts denounced, in accordance with the evidence of

that is available, the Data Inspection of this Spanish Agency for the Protection of

Data, considers that the treatment of personal data that is carried out by the

entity claimed does not meet the conditions imposed by the regulations on

data protection, so it is appropriate to open this procedure

sanctioning

FIFTH: On June 7, 2021, the Director of the Spanish Agency for

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

alleged infringement of article 32 of the RGPD and 5.1.f) of the RGPD.

SIXTH: Having notified the aforementioned initial 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.

In view of everything that has been done, by the Spanish Agency for the Protection of

Data, in this procedure, the following are considered proven facts,

FACTS

FIRST: On October 6, 2020, the claimant files a claim before

the Spanish Agency for Data Protection, against the CLUB NÁUTICO EL ESTACIO,

since said entity has published on its website, the call and the Minutes of the

Ordinary Meeting of the Club, exposing your personal data, without restrictions of

access.

SECOND: Checked that both documents are accessible on the web

of the entity, a response is received from the respondent in which, in summary, he highlights

manifest that was placed on the bulletin board and on the web page as always

Has made.

FOUNDATIONS OF LAW

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.

Yo

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 offers clear indications that the

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

relation to article 5 of the LOPGDD, duty of confidentiality, when publishing in its

web, the call and the minutes of the ordinary Board of the Club, disclosing information and

personal data to third parties.

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.

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

of the treatment", establishes that:

III

"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.

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”.

IV

From the documentation in the file, there are clear indications that the

claimed has violated article 32 of the RGPD, when an incident of

security due to the publication on its website of personal data of the

claimant, allowing 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/08576/2020, the AEPD transferred to the respondent, the claim submitted for analysis, requesting the provision of information related to the incident. Of the documentation provided, the respondent states that it was placed on the notice board ads and on the website as it has always been done.

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, it is estimated that the respondent is responsible for the infringement of article 32 of the RGPD, infringement typified in article 83.4.a) of the GDPR.

Article 83.5 of the RGPD provides the following:

v

"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.

In order to determine the administrative fine to be imposed, the

provisions of articles 83.1 and 83.2 of the RGPD, precepts that indicate:

SAW

"1. Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

Regulation indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or as a substitute for the measures contemplated in the

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the nature

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to pa-

allocate the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment,

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the person in charge or the person in charge of the treatment;

f) the degree of cooperation with the supervisory authority in order to remedy the

infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in particular

whether the person in charge or the person in charge notified the infringement and, if so, to what extent.

gives; i) when the measures indicated in article 58, section 2, have been ordered

given previously against the person in charge or the person in charge in question in relation to

the same matter, compliance with said measures;

j) adherence to codes of conduct under Article 40 or to certification mechanisms

approvals approved in accordance with article 42,

k) any other aggravating or mitigating factor applicable to the circumstances of the case,

such as financial benefits obtained or losses avoided, directly or indirectly.

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"1. The penalties provided for in sections 4, 5 and 6 of article 83 of the Regulation

(EU) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of the aforementioned article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatments

of personal data.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission of the offence.

e) The existence of a merger by absorption process after the commission

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

h) The submission by the person in charge or person in charge, with

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any

interested."

data.

In accordance with the precepts transcribed, in order to set the amount of the penalty for infringement of article 5.1 f) and 32 of the RGPD, to the CLUB NÁUTICO EL ESTACIO, as responsible for the aforementioned infractions typified in articles 83.5 and 83.4 of the

RGPD, it is appropriate to graduate the fine taking into account:

-The scope in a local environment of the treatment carried out by the entity claimed.

-The number of affected is limited to a single person, the claimant.

-There is no evidence that the entity had acted maliciously, although the performance reveals a serious lack of diligence.

-The claimed entity is a small business.

Considering the exposed factors, the valuation that reaches the amount of the fine is €2,000 for violation of article 5.1 f) of the RGPD, regarding the violation of the principle of confidentiality and €1,000 for infringement of article 32 of the aforementioned RGPD, regarding the security of the processing of the personal data of the claimant.

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:

7th

"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."

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 CLUB NAUTICO EL ESTACIO, with CIF G73044893, for a

infringement of article 32 of the RGPD, and article 5.1.f) of the RGPD, typified in the article

83.5 of the RGPD, a fine of €3,000 (three thousand euros).

SECOND: NOTIFY this resolution to CLUB NAUTICO EL ESTACIO.

THIRD

: Warn the sanctioned person that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following month or immediately after, and if between the 16th and last day of each month, both inclusive, the payment term It will be until the 5th of the second following month or immediately after.

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

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es