938-0419

Procedure No.: PS/00326/2018

RESOLUTION OF PUNISHMENT PROCEDURE

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

the following

BACKGROUND

FIRST: On June 11, 2018, the director of the Spanish Agency for

Data Protection agrees to initiate these investigative actions aimed at

to clarify the facts in relation to the news that appeared in the press about the possible

Violation of data protection regulations by the National League of

Professional Football and the application for mobile devices of La Liga. (appLALIGA or the

application hereinafter).

Likewise, on June 19, 2018, this Agency received a letter from FACUA

denouncing the National Professional Football League on the occasion of the creation by

of that entity of a mobile application that can indiscriminately capture sounds

environments of the place where the user is.

They indicate that collecting ambient sound in catering establishments may imply

capturing conversations that may reveal personal data of third parties

people who have not given their consent for the processing of said data by

any means, which would be particularly burdensome if such talks could

hold specially protected data.

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

preliminary investigative actions to clarify the facts, taking into account

knowledge of the following extremes:

1. The following checks have been carried out by the Data Inspection

in relation to the LALIGA app:

1- On 06/12/2018, the LALIGA app was installed on a phone

Mobile Data Inspection.

2- According to the information shown in the Google Play Store, it is a

version dated June 8, 2018, the LALIGA app having been published by

first time on February 29, 2012.

3- Once the installation is done, it is verified that the message of

correct installation. The LALIGA app is executed, checking that the

initial screens of the application, which show the “GENERAL CONDITIONS

OF USE AND PRIVACY POLICY”, stating as responsible “National League

of Professional Football”.

It is indicated that it is a summary, which occupies a total of four pages of the

mobile, and containing a link to "LaLiga's privacy policy"

(https://www.laliga.es/aviso-legal-privacidad-cookies/).

A button “I have read it” appears, verifying that until this button is pressed, the

you can continue to run the application.

a.

4- Once the “I have read it” button is pressed, a screen with two boxes appears

to mark two acceptances:

“I have read and accept the Legal Conditions and the Privacy Policy of the

AppLALIGA <<link to the aforementioned information>>,

confirming that I am over 14 years of age, and specifically that LaLiga treats my

personal data to offer me information related to competitions

that organizes through the AppLALIGA …”

It is necessary to clarify that the content of the "related information" refers to dates,

hours and result of the matches that are held by the member clubs of the

association LA LIGA, and which is also accessible through the website www.laliga.es

and therefore, without the need to download and install the LALIGA app.

b.

“Protect your team! By clicking here, you accept that LaLiga processes your data

personal, including those obtained through the microphone of your device

mobile and geopositioning, to detect fraud in the consumption of football in

unauthorized public establishments.

5- It has been proven that progress cannot be made if the

“APPLALIGA Legal Conditions and Privacy Policy”. It has been

also verified that, if at that point you exit the application and return to

to enter, the LALIGA app shows the same screen again, which prevents continuing

with access to the application until the aforementioned conditions are accepted.

6- It is verified that the application can be accessed by checking the box

acceptance of the "Legal Conditions and the Privacy Policy of the

APPLALIGA” and not the acceptance of personal data processing

obtained through the microphone of the mobile device and geopositioning,

for the purpose of detecting fraud in the consumption of football in

unauthorized public establishments. It is accessed without accepting the treatments

of the data obtained from the microphone and the location.

7- It is verified that the application is installed and apparently in

operation on mobile phone. It is verified that the "Conditions

Legal and Privacy Policy", are also accessible in the tab

LEGAL CONDITIONS of the application.

8 - The LALIGA app is uninstalled (previously installed on the day

06/12/2018), and is reinstalled on 06/15/2018.

C/ Jorge Juan 6

28001 - Madrid

http://www.aepd.es

https://sedeaepd.gob.es

3/85

9- The LALIGA app is executed verifying that the Conditions are displayed

Legal. On this occasion, the treatment of the data obtained by the user is accepted.

microphone and geopositioning of the device.

10- It is verified that pop-up screens are additionally shown

independents requesting permission to record audio and access location on

telephone.

11- Once in the application, no icon is observed (not found) in the

application that shows the activation of the microphone or the location, or icons or

marks that reflect the authorization for its possible activation. I do not know

find information about the status of these activations within the

application options and menus.

12- The application is exited and the administration option of

Android operating system applications, verifying that they are active

the microphone and location for the LALIGA app. It is verified that they can be deactivated.

2- On 06/21/2018 an inspection is carried out at the NATIONAL FOOTBALL LEAGUE

PROFESSIONAL (hereinafter THE LEAGUE). The representatives of the entity carry out the

following manifestations:

1- As reported in the press release dated 11

June 2018, with the aim of protection against fraud that occurs with

the broadcasting of football matches by public establishments that do not

hold the corresponding permits, and which represent an estimated loss of

150 million euros for Spanish football, LA LIGA has implemented a new

functionality in its official LALIGA app with the sole objective of detecting these

fraudulent exploitation.

This functionality will be used both in the days of the Official League of first and

second division and the Copa del Rey, for which establishments need

emission permit, that is, those included in the HORECA lot.

2- This new functionality for fraud detection is enabled in the

appLALIGA since last Friday, June 8, 2018, only for users of the

Android system version 6.0 for its specific management of permissions) or higher

and at the national level. This functionality uses pickups from the microphone of the

mobile device and its location.

There are about 10 million users of the LALIGA app. However, it has

enabled a limit of 50,000 users nationwide (only for Spain),

maximum number of installations with this new functionality, which they estimate

sufficient as a sample for the intended purpose. Outside of Spain it is prevented

this functionality.

This functionality has been used only during the initial days of

the playoffs of the National League, on June 9, 2018. On June 9, the

proceeded to the suspension of the functionality due to the multiple news

published about the LALIGA app that included strategic aspects of its

operation, with technical risk, as well as by the social alarm aroused.

3- Users are informed of the new functionality through the Conditions

General Terms of Use and Privacy Policy that are displayed when installing the

appLALIGA, requesting their acceptance. Otherwise the

appLALIGA stops its execution. A link to the Privacy Policy is included

complete LALIGA environment.

In order for the microphone and location data to be processed for the stated purpose,

the user must give his consent expressly accepting said

treatments, checking the box enabled for this purpose after reading the

General Conditions of Use and Privacy Policy.

4-The LALIGA app works as follows:

c. A. When a user downloads the LALIGA app, the operating system of

your mobile device asks you, through pop-up windows, to provide

your consent so that THE LEAGUE can activate the microphone and the

device geolocation.

d. B. The LALIGA app does not have a user registration process such as

such, during which they must provide some type of name, username or

identify yourself by providing any type of data.

Yes, the IP address of the device is recorded at the time of installation

and a specific identifier assigned by the LALIGA app to the user

(LALIGA app installation identifier).

The user agent whose content depends on the manufacturer is also collected, and

which usually includes the version of the operating system.

and. C. Only if you choose to accept, the microphone will pick up binary codes of

audio fragments, with the sole purpose of being able to know if the user

You are watching football matches of competitions played by teams from

LA LIGA, but the content of the recording will never be accessed.

The location of the device is also recorded for comparison with the

location of catering establishments.

F. D. For the treatment of the captured sound, the ACR technique is used

(Automatic Content Recognition) called LA audio fingerprinting

COMPANY 1 consisting of the analysis of the intrinsic characteristics of the

audio and its filtering, and generating a binary hash that will form the fingerprint

of the audio.

This process is done entirely on the user's mobile device

through the technology of THE COMPANY 1 integrated in the AppLALIGA. The

AppLALIGA stores the fingerprint generated in the internal memory of the

user's device, discarding the audio, in such a way that it is not

generates any file that is stored in any directory of

device storage and that may be accessible by other

applications or the operating system, and that contains, or the audio captured by

the microphone, nor the fingerprint generated.

On the other hand, from the generated footprint it is not possible to obtain the audio

that was captured, due to the lossy encoding performed by the

hash algorithm used.

That is, the captured audio fragments are encoded in the

phone automatically through an algorithm that does not allow reversing

the process, in such a way that, once the sound capture

made by the microphone, its reversal is impossible and the audio cannot be

be obtained again.

The fingerprint obtained is sent through an https connection (encrypted) to the

company THE COMPANY 1, with whom LA LIGA has signed a contract of

provision of services dated March 23, 2018, a copy of which is in

inspection actions.

COMPANY 1 receives fingerprints from mobile devices

of users and compares them with the fingerprints generated in real time

from the audios of the broadcasts provided by LA LIGA.

COMPANY 1, in order to make an effective comparison, carries out a series

of signal treatments consisting of the transformation in frequency

of the audio signal and obtaining, on the frequency signal, a

series of characteristics of the signal on which the analysis is carried out.

comparison, using its own technology.

If it does not match, the fingerprint is deleted and is not preserved.

The number of comparisons made is configurable to give greater

reliability.

g. E. LA LIGA has a database of public establishments

HORECA.

COMPANY 1, by virtue of the signed contract, has collaborated with the

Business Intelligence Department of LA LIGA with the personalization and

adaptation for integration with coordinate information

(Location).

The reception of the location is done on a computer server in LA

COMPANY 1, receiving the latitude and longitude via https (encryption)

(location) as well as a timestamp, the user identifier

assigned by the LALIGA app and the IP address of the device.

From the trace a CSV is generated that is sent to the department of

LA LIGA Business Intelligence for analysis.

Since the location does not collect the height parameter, it cannot be

determine if the user is in a bar on the street or in a

private residence or dwelling located at any height in the same

portrait of the establishment.

The Business Intelligence department analyzes information from

the CSVs of both the acoustic footprints and the locations and the base

of HORECA data, determining the possible actions against the

establishments likely to be committing an act

fraudulent.

Work in the present inspection actions copy of traces and CSV

generated both for the traces generated from the audios and

for the locations.

h. F. With this procedure it can be ensured that no person or

user, neither from LA LIGA nor external to the entity, can access the

sound captures made by the microphones, but only to a few

alphanumeric codes -the fingerprint-, since the audios are transformed into

the user's own mobile device.

The only treatment carried out with these codes is their comparison with

other reference codes in order to determine the presence of a

television with a broadcast of a football match in the vicinity of the

microphone.

Yo.

J. H. In order to minimize the processing carried out, LA LIGA only

activate the microphone and location (using GPS positioning, in

forward geopositioning) of the mobile device during the fringes

schedules of matches in which LA LIGA teams compete.- It is necessary

clarify that this information does not appear in the informative legend that

appears in point 1.4 of the second antecedent of the initiation agreement, which

is the one that is available to users when they download and install

the application, that is, there is no reference to the moment in which

Activate the aforementioned functionalities. Specifically in the summary of the

general conditions of use and privacy policy, which are shown when

user when downloading and installing the LALIGA app, in section 3 USE

OF THE MICROPHONE and in section 4. USE OF GEOPOSITIONING

This information is not expressly stated.

Prior to the development of the new functionality of the application,

THE LEAGUE requested two legal reports (LAWYERS 2 and LAWYERS 1)

for the study of the possible implications of data protection.

Internal Privacy by Design meetings were also held.

k.

from the Design) on the AppLALIGA that are documented, and

an analysis of the need to carry out an Impact Assessment and Analysis

of Risks.

In the implementation of the LALIGA app, we have taken into account the

considerations derived from these legal reports.- It is necessary to clarify

that in one of the requested reports it is proposed as a safeguard to

take into account in order to comply with the regulations for the protection of

data, that the user is informed of the activation and use of the aforementioned

functionalities, and yet of the actions carried out and with the

elements that appear in them, it does not follow that on the part of

THE LEAGUE have been taken into account.

LA LIGA considers that the option of capturing a signal through the

microphone is not intrusive, since as has been commented, through the

solution adopted recordings are not or cannot be accessed

conversation sounds.

I. The user can revoke their consent at any time in the

mobile device settings. Within the LALIGA app there is no

option available to the user to disable the microphone or the

geopositioning.

The LALIGA app also does not show any icon or mark indicating that the

microphone or geopositioning is active or in standby

possible activation or that indicates as a reminder that the user gave

your consent at the time.

As indicated in the Conditions, LA LIGA will periodically remind

to the user with a determined periodicity that can activate its

microphone and geopositioning, and requesting that you confirm your

consent again. – It is necessary to clarify that in the device in which

that the LALIGA app is downloaded, this information does not appear, since it shows a

summary of the conditions that this end does not include and that are referred to

a link on the www.laliga.es website that must be accessed

expressly to know that information. -

Only five requests have been received to oppose these treatments.

l.

J. Regarding the Privacy Policy published on the website of

LA LIGA (www.laliga.es), the referral made to users of the

appLALIGA is for the purposes numbered 1 and 5.

m. K. Regarding the segmentation of profiles that appears in purpose 4 of the

Privacy Policy published on the website, has not been made in

no time.

n. L. No age verification has been performed on users who

have downloaded the LALIGA app.

either. M. The LALIGA app does not use any type of cookies.

1.

Examined the contract dated 03/23/2018 signed between LA LIGA and LA

COMPANY 1, it is verified that it establishes, in “ANNEX II. AGREEMENT OF

PROCESSING OF PERSONAL DATA” the following:

1-The person in charge of the treatment, THE COMPANY 1, will only process the data

in accordance with the instructions of the controller, LA LIGA, the only one that

will decide on the purpose, use and data processing systems.

2- THE COMPANY 1 will not apply or use the data for a purpose other than that which appears in

said contract, nor will it communicate them to other people.

3- The security measures corresponding to a basic level are stipulated,

being the

implement them,

committing the person in charge to include in his security document a

reference to them.

4- Once the contractual provision has been fulfilled, the personal data

they must be destroyed.

5- There is a commitment to sign, before May 25, 2018, an agreement

data processing order that complies with the RGPD 2016/679.

forced treatment to

in charge of

two.

It is signed on 05/24/2018 between LA LIGA and LA COMPANY 1, this

new contract of order of treatment referred to the RGPD, whose copy works in the

these inspection actions and provides, among other aspects:

1- Object, duration, nature and purpose of the treatments, as well as the type of

personal data to be processed of the users of the LALIGA app.

2- Obligation of the person in charge of processing personal data only following

documented instructions of the person in charge and exclusively when

necessary for the provision of services.

3- Conditions for the person in charge to give their prior authorization,

specific or general, to subcontracting

4- Assistance to the person in charge in the attention to the exercise of rights of the

interested parties, transferring to THE LEAGUE the applications received by COMPANY 1 to

regard.

5- Notification of personal data security violations.

6- Security measures that COMPANY 1 must comply with, described

in ANNEX I.

1)

In relation to the previous study carried out by LA LIGA:

1- Work in the inspection actions a Report prepared by LAWYERS

2, dated 07/14/2016, in which the technology used by LA is analyzed

COMPANY 1 and its adaptation to data protection regulations.

This report incorrectly indicates that when the LALIGA app is not

is running, there are no captures. However, during the

inspection carried out, it was revealed that the withdrawals occur

Once the LALIGA app has been installed on the mobile device (and the

consents), even if the LALIGA app is not running

spotlight. As stated above, this means that in the

device screen does not appear as “open or working” the

mentioned application – that is, in the foreground-, being able to appear on the screen

of the device the “home screen” or the “lock screen” that the user

you have arranged in the customization options, it could even appear in the

screen another application that is currently being used, and despite

Therefore, the LALIGA app could be collecting and, where appropriate, sending

information. - that is, running in the background.

2- There is also a legal report from LAWYERS 1, dated April 2018,

on the use of audio capture functionalities and location of the

appLALIGA. In the report, for both audio and video purposes,

geopositioning, a set of safeguards are proposed, including:

1. Obtain the user's consent and follow the principle of privacy by

default (privacy by default), expressly authorizing the user to

functionality.

two.

Inform the user in a simple but exhaustive way about the

characteristics of the recordings. The user must be able to wait

reasonably what is the scope of the treatment that will be carried out

cape.

3. Establish restrictions on the use of the functionality, limiting

temporary spaces and previously informing the user. For example:

when matches organized by LA LIGA are being played.

4. The LALIGA app must display notices or warnings to remind

frequent way to the user that the sensors are collecting their data

personal.

5. Periodically renew the consents.

6.

Include in the LALIGA app a specific icon by which the user can

know when LA LIGA collects audio and location.

7. Facilitate a simple system to revoke consent, proposing

include a specific box in the settings or configuration menu of the

appLALIGA.

3- Work in the inspection actions copy of documentation that reflects the

internal meetings in LA LIGA of Privacy by Design about the AppLALIGA,

maintained in March 2018. In this documentation it is recommended

anonymize the data obtained in such a way that it cannot be associated with any

personal data or identifier. Specifically, it is recommended not to treat or collect

unique identifiers such as IMEI, MAC address, device id, ID of

advertising, device serial number or IP address.

4- Documentation related to carrying out an analysis of the need for

carry out an Impact Assessment, in relation to the new functionality of the

appLALIGA. They are collected as measures for the treatment of risks, among

others, the following:

8. Update of the “GENERAL CONDITIONS OF USE AND POLICY

OF PRIVACY". Updated May 25, 2018.

Inclusion of independent checkboxes.

9.

10. Offer the possibility of separate consent to treat the data with

other purposes.

11. Allow the use of the LALIGA app without user registration, as

does

After examining five opposition requests received by LA LIGA, the following is verified:

two)

Next:

1- The requests focus, in particular, on how to revoke consent

for the microphone and geopositioning functionalities, that is, on how

deactivate the geolocation and microphone functions. of these requests

it could be deduced that users have not found in the LALIGA app a

procedure for the revocation of the consent they granted when

downloaded and installed the aforementioned application. -This absence of procedure for the

revocation in the application itself is recognized by the representatives of LA LIGA

in the actions carried out and proof of said non-existence is the answer that

receive the following users:

2- All users are answered indicating that they can revoke their

microphone access permission consent by accessing on your phone to:

“Settings” > “Applications” > “Permissions” > “Microphone” and deactivating said option.

This shows that the only option to revoke consent is to go

the configuration options provided by the device's operating system,

when there is a procedure at the time of giving consent

implemented ad hoc in the application itself.

THIRD: On December 12, 2018, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the NATIONAL LEAGUE OF

PROFESSIONAL FOOTBALL with NIF G78069762 in accordance with the provisions of articles

63 and 64 of Law 39/2015, of October 1, of the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP), for the alleged infringement of the

article 5.1 a) of the RGPD, provided for in article 83.5 a) of the aforementioned RGPD and for the alleged

infringement of article 7.3 of the RGPD, provided for in article 83.1 of the aforementioned RGPD.

FOURTH: In the aforementioned Initial Agreement it was agreed (...) TO INCORPORATE in the file

sanctioning party, for evidentiary purposes, the claim filed by the claimant and its

documentation, the documents obtained and generated by the General Subdirectorate of

Data Inspection during the investigation phase, as well as the report of

prior inspection actions. (…)

(…) THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of October 1, of the

Common Administrative Procedure of the Public Administrations, the sanction that

could correspond due to violation of article 5.1 a) of the RGPD would be the imposition of

a pecuniary fine to the claimed entity, in the amount of 200,000 euros (two hundred

thousand euros), without prejudice to what results from the instruction.

THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations, the measure

corrective measure that may correspond due to violation of article 7.3 a) of the RGPD would be

order the claimed entity, so that within ONE MONTH proceed to the

establishment of a consent revocation procedure in the terms

indicated in article 7.3 of the RGPD (...)

FIFTH:

He presented a pleadings brief in which, in summary, he stated the following:

Notified of the aforementioned start-up agreement, on 01/24/2019, LA LIGA

First. - Lack of legitimation of FACUA. –

Second. – the actions take place in the context of the fight against piracy and

therefore on the basis of a legitimate interest.

The investigated entity alleges that it had great diligence and demonstrated responsibility

proactive, as I request two reports from external experts and their intention to

collaborating always with the AEPD was always present. He also named a

Data Protection Delegate despite not being obliged to do so. and were held in

takes into account the recommendations of the reports weighing the interests at stake and

establishing a calendar of improvements that would be implemented gradually.

The implementation of some recommendations was replaced by an improvement

technique of the technology used, making irreversible the audios that are

they captured Being transparent at all times and showing caution and diligence in the

compliance with the principles of legality, loyalty and transparency.

Third. – On compliance with the duty to inform ar. 13 GDPR and principle of

transparency art. 5.1 GDPR.

3.1 on the operation and the data anonymization process.

A reference is made to what was indicated in the inspection. Emphasizing that the

Consent is given twice: in the app itself and another through the system

device operation. If they have not been accepted, the functionalities are not activated,

therefore requires a double opt-in. Regarding the functionality of the microphone, it is alleged

identical terms to what was stated in the inspection, indicating that the transformation of the

audio content in a fingerprint is unintelligible, irreproducible and irreversible and,

does not allow to recognize the original content. It is then sent to COMPANY 1 and compared in real time with the broadcasts of the matches. Therefore it is not possible to access to the recordings made, the final result of the treatment being the anonymization of audio data, so the data protection regulations would not apply according to Recital 26.

Given the anonymization of the data, the impact on the rights and freedoms of the user for the treatment of the data is null, and therefore does not have characteristics that require a special adaptation of the elements of the principle of transparency, since it is not subject to data protection regulations.

Regarding the location, LALIGA decided that the basis of the treatment would be the express consent of the user, and it was done in two moments, as has been said about the microphone.

The operating system of the device itself shows, by default, an icon on the notification bar at the time of location, as is the case in many other applications on the market that make use of the device's geolocation. In the diligence of 06/15/2018 this extreme is appreciated, therefore, the principle of transparency. The certificate containing the navigation record carried out on the 01/20/2019 demonstrating the activation of an icon and an attachment referring to a video where at minute one and fifty-five seconds appears in the bar notifications the activation of the geopositioning functionality, remaining active during the time it is being collected.

In short, the principle of transparency has been complied with despite the fact that the

treatment does not require its own characteristics that require a special adaptation of

the elements of the aforementioned principle.

3.2 About the identification of personal data collected through the

microphone functionalities and geopositioning of the app.

It should be noted that the user agent was not linked to any personal data

of the user beyond the IP address and location, which was necessary to be able to

pair it with the device and ensure that the permissions granted by the device were applied.

user to the app. The treatment of the IP address and the user agent of the

device. The specific identifier assigned by the application to the device allows

relate the data obtained, without being able to link to a specific user.

Geolocation data is not intrusive since it does not deal with location

of the user's mobile device, but transforms said information into a

heat map, identifying the sections of the territory in which more frauds are

detected, which is then checked against the database of public establishments

HORECA. In conclusion, the data collected is anonymized and is not

are subject to data protection regulations or are adequate,

pertinent and for the fulfillment of the purpose for which they were collected.

In order to reinforce the principle of transparency, when development allowed it,

stopped treating both the IP of the device and the user agent, notwithstanding that this

would suppose a loss of extra control of verification of the scope of the treatment.

3.3 Moment in which the consent is obtained, the fulfillment of the duty of

inform and the principle of transparency in the complementary information provided to the

interested.

3.3a). Regarding the moment in which consent is obtained, it is indicated

that LALIGA previously obtains the consent of the interested parties, and given the

treatment, it is not considered that it has special characteristics that require

an adaptation of the aforementioned principle. The interpretation of the AEPD would lead to, in each

treatment operation or activity, (see normative definition) it would have to be informed and

request again, which would be impossible in practice and hinders the normal

execution of any processing of personal data necessary to achieve the purposes

legitimate of the person in charge.

3.3 b) Compliance with the duty to inform and the principle of transparency.

Regarding the two differentiated moments:

1 When consent is given for treatment, the AEPD understands that

there are shortcomings as evidenced in the initial agreement, however, that

information is provided in the privacy policy of the app made available both

at the time of collecting consent and permanently in the

"Legal Conditions" section of the app menu, the specific publication of

the conditions of June 9, 2018, in identical terms occurs with the space

time in which the functionalities were activated.

Although it is true that both the information regarding the moment in which

functionalities such as information related to the impossibility of

pick up conversations from the environment do not appear in the basic information that constitutes

the first layer, neither in the guide for compliance with the duty to inform of the AEPD nor

in art 11.2 LOPDGG they point out aspects in that sense, that is, include information

regarding the moment in which the effective treatment of the data will take place, nor the

limitations that have been established to said treatments.

Despite this non-enforceability, LALIGA includes in the first layer the information

minimum required and also two different and independent sections in which

informs about the mentioned functionalities. (3. Using the microphone and 4. Using the

geopositioning)

In conclusion, they consider that they fully comply with the duty of

transparency regulated in arts. 12, 13 and 5 of the RGPD and 11.2 of the LOPDGG, as well as

the guidelines published to date by the supervisory authority in relation to the

information regarding the moment of activation of the microphone functionalities and

geopositioning.

2 when the treatment of the same is executed and the reminders on the

treatments performed.

At the moment in which the microphone functionality is activated, no data is collected

personal information, so that said demand for information cannot be based on an obligation

any derived from compliance with the regulations. The only purpose for which

would alert is that the resources of your mobile device are being used, but not

process your personal data.

LALIGA understands that including an additional icon to all the information already provided

would be excessive, it would not provide additional guarantees for the protection of rights and

freedoms and would be invasive for users by including images on devices

that could be annoying, generating a false perception that it is being recorded

the voice and the conversations that are taking place around the device, giving rise to

to an unnecessary social alarm.

Regarding the geolocation functionality, the device shows, for

default, an icon in the notification bar at the time of capturing the

location, as stated in the video provided as document No. 3.

Periodic reminder of activation of the microphone and geopositioning of the

mobile device.

The AEPD indicates that it is not reported in the summary of the conditions that appears

at the time of download and installation about the reminder that will be made to the

users. As indicated before, there is no legal obligation in this regard. Nope

Notwithstanding the foregoing, LALIGA provides this information through the policy of

privacy of the app that is provided both at the time of installation of the application

and permanently in the "legal conditions". likewise, since

the application was only used on June 9, it could hardly have been sent

no reminder.

3.4 Regarding the relationship between the principle of loyalty and the principle of transparency of the

GDPR.

3.4.a) The effectiveness of the application in its fight against fraud is out of

any doubt, since it helps to (i) detect and prevent illegal emissions, (ii) facilitates

tracking and detection of public establishments that emit the signal

fraudulently and (iii) optimizes resources deployed by LAIGA.

3.4.b) On the added value to the users of the application with respect to the page

Web.

The app and the web have different objectives. The app seeks to generate a greater

link between the user and the entity and shows a content adapted to a

concrete need. And it shows additional content such as personalization by

favorite team, the presentation of content, the sending of notifications within the

own app, maps to guide to the stadium, and connectivity with other applications of

THE LEAGUE. In short, they are different means of communication, on the web you can

find elements that are accessed with the app, but in this there are other contents

additional.

3.4. c) On the processing of data for a purpose other than the main one: the

app informs of the possibilities of accessing the functionalities, and if so

is accepted, with a legitimate purpose, not being mandatory the acceptance of this

treatment to continue with the full use of the app.

The processing of data for a purpose other than the main one is permitted by the

regulations as long as there is a valid basis of legitimacy and, where appropriate,

Specific and independent consents are requested for each of the

purposes if they are incompatible with each other. (considering 50 and 61 RGPD). So that

The processing to combat fraud cannot be considered unlawful because of the

fact that it is a different purpose from the main one.

In view of the foregoing, it can be concluded that the principle of

transparency and therefore is violating the principle of typicity that governs the right

sanctioning

Quarter. - on the infringement of art. 7.3 RGPD regarding the revocation of the

consents given.

The revocation procedure is not limited only to the system

operating system of the device where the app is installed, but it is also available the

email address lopd@laliga.es. However, a panel of references has been included

privacy within the app menu called "subscription center" that

allows the revocation of the consents given, as well as its new collection.

Facilitating the revocation through the marking of a box, in the same terms

than at the start. Documentation is provided proving the existence of said

process. At the time of inspection in June 2018 it was under development,

being effectively implemented during the month of September.

There is no evidence that any user has not been able to revoke their consent through

of the operating system configuration.

Fifth. - on the mitigating and aggravating circumstances of art 83.2 RGPD.

5.1 Mitigations.

It has acted diligently at all times, and if it has been the opposite,

due to an erroneous interpretation of the principles introduced by the new regulations,

but without the intention of achieving an end at the expense of the violation of the rights of the

affected. There is no budget that can carry out a sanction and there is no

have correctly appreciated in the agreement the concurrent elements in the present

case. It is mentioned that only one extenuating circumstance has been taken into account referring to the

duration of the infraction, however, there are others:

-The adoption of appropriate measures to mitigate possible damage and

damages by developing the app from the principle of privacy by design and by

default, self-imposed diligence and proactive responsibility. This mitigation is

corresponds to art. 83.2 c) GDPR. “Any action taken by the person responsible or

in charge of the treatment to mitigate the damages suffered by the interested parties”

-The volume of affected subjects. The 50,000 users cannot be a

large-scale number for its management of a supposed base of 10,000,000 possible

users. The figure obtained from Google Play does not allow us to infer the number of users who

have active the functionalities or the operating system that was required to be

Android 6.0 or higher. This attenuation corresponds to art. 83.2 a) GDPR.

-LALIGA has not committed any previous infraction regarding the protection of

data, this mitigating factor corresponds to art. 83.2 e) GDPR.

-LALIGA has cooperated proactively with the AEPD from the very beginning.

both through tweeter and by sending emails addressed to

instruccion@agpd.es and inspeccion@agpd.es. Likewise, during the inspection visit,

showed a collaborative attitude, with the presence of COMPANY 1 in order to provide

of maximum transparency to the procedure. This circumstance corresponds to the

art. 83.2 f) GDPR.

5.2 aggravating circumstances appreciated by the AEPD to the alleged infringement.

Regarding the provision in art. 83.2 RGPD, the AEPD considers the nature of the

violation of an essential reporting principle such as transparency. Without

However, it was complied with at all times as explained during the writing of

allegations. Similarly, this provision would not apply to the

“number of affected”, taking into account that there were a maximum of 50,000 users. The

concept of “large scale” offers orientations and WP 243 rev.01 also, to which

makes the appropriate referral where it cannot be applied to users affected by

the application

-those relating to letters b) and d) of the aforementioned precept. contrary to what is appreciated

by the AEPD, LALIGA strictly complied with the reports requested from the

law firms. The measure that was not implemented in the opinion of the AEPD was the

regarding the incorporation of an icon that reminds us of the activation of the functionality of the

microphone. Remembering in this sense that personal data is not processed, therefore

that such incorporation was not considered necessary and the Android operating system itself

emits an icon that is visible in the notification bar every time it is

activate the geo position functionality. Therefore, LA LIGA considers that the AEPD does not

has not taken into account, nor has it assessed compliance with the rest of the recommendations, nor has

have considered the other circumstances.

On the application of letter k) of the aforementioned precept:

The AEPD considers that this circumstance is applicable as an aggravating circumstance, for

when it pursues “exercising its interest in protecting its financial assets from fraud”. Nope

It can be forgotten that one of the purposes of the data processing carried out by the app

is the detection and prevention of fraud, which constitutes a legitimate interest under the

Considering 47 of the RGPD. Protect the assets of the entity, in terms of rights

audiovisual, results in culture and the economy actively fighting against the

scourge that is piracy.

This purpose cannot hide the fact that it will have an economic impact on the asset.

Of the entity. But the social relevance of the asset of the company must be taken into account.

entity (which exceeds the professional field of soccer, since with the income of the

entity contributes to legally established solidarity mechanisms such as (i)

the Compensation Fund of the sports entities that, disputing the competition

from professional soccer, they descend from category; (ii) for policies to promote the professional and amateur soccer competition; (iii) for the policies of the Board of Governors of Sports in support of the First Division of Women's Soccer, Second Division B of the Men's National Championship and the associations of soccer players, referees, trainers and physical trainers) and the general interest of protecting and conserving such audiovisual rights. LALIGA does not focus its work solely on protecting audiovisual rights, but also maintains a very proactive, collaborative and cooperative attitude advice to the most diverse organizations and authorities at the national and internationally, fighting against all possible fronts, including the judicial ones against this great endemic evil that devastates the culture of the countries.

Sixth. - On the aggravating circumstances of art. 83.2 RGPD, which graduate the sanction related to the violation of art. 7.3 of the GDPR. The AEPD considers applicable the aggravating circumstance of art. 83.2 a) RGPD because the number of users of the application and the time during which the form of obtaining and revoking consent remains in force.

The figure obtained from the Google Play Store does not take into account the real volume of active users of the application, since it takes into account the downloads of the application since 2012 and those who have been able to deactivate it before the 8th of June 2018- date on which the new functionalities were published- . likewise, It should also be noted that the function is only enabled for users with Android 6.0 or higher operating system. As for the time of the infraction, you must indicate that the "subscription center" is effectively implemented during the month of September 2018. Therefore, the time elapsed without been able to count on the aforementioned "Subscription Center" is limited to the months of June, July and August, which coincides with the competition break. The application of the letter b) referring to intentionality or negligence in the infringement. The implementation of Subscription Center, developed since May and finally implemented in

September, cannot be considered as an aggravating circumstance, given that no

committed any offence.

Seventh. - on the sanction proposal.

In the start-up agreement there have been no other extenuating circumstances that

present in this case:

The non-existence of a profit motive; the absence of a complaint filed by

affected; the absence of previous violations; the null intentionality; the taking of

immediate measures at the time of knowing the news, temporarily suspending

the functionalities; the degree of cooperation with the AEPD. the only circumstance

mitigating factor included in the initiation agreement is that relating to the duration of the infraction by

when the functionalities were used on 06/09/2018, but the degree to which is not determined

that it has an impact on the sanction proposal. According to art. 76 LOPDGG, should

take into account the previous extenuating circumstances that reduce

considerably the amount of the sanction, all in accordance with art. 29

LRJSP, by virtue of which the due suitability and necessity of the

sanction to be imposed and its adequacy to the seriousness of the act constituting the infraction.

The administrative authority should especially consider the following

criteria:

a) The degree of culpability or the existence of intent, which has been

shown that there is no place.

b) The continuity or persistence of the offending conduct, which is not

for circumscribing the facts to the day 06/9/2018.

c) The nature of the damages caused, which have not existed or been

accredited.

d) Recidivism, which does not apply to this case.

LALIGA do not find objective justification in the initiation agreement about why

why it is decided to impose such an amount and not a smaller one or, for example, a warning.

For all of the above, it requests the filing of the proceedings without the imposition of

any penalty.

SIXTH: In accordance with the provisions of article 77 of Law 39/2015, of 1

October, the following tests were carried out:

a) On the date of 02/07/2019, the Data Inspector was requested to carry out the following

Test:

Installation of the LALIGA application on a mobile device with an operating system

1-

Android version 6, or higher for verification purposes:

The information offered during the start of the installation. (both on the device,

how if a link to another web page is displayed)

The request for permits/consents.

The existence of a user subscription procedure.

two-

effects of checking:

The information displayed on the device screen regarding the existence of

icons or notices of the use of geolocation and use of microphone.

In case there is a procedure through registration and user, proceed to the

yourself and verify the services offered.

3-

use of the microphone and geolocation functionalities, in order to verify:

The request for the exercise of opposition or the revocation of the consent of the

The use of the LALIGA application in conferences organized by LA LIGA, to which

The procedure authorized for this purpose by LA LIGA.

a. The result was incorporated as a procedure dated 02/11/2019, which was

transcribed below, (without the corresponding screenshots

contained in the aforementioned diligence):

To record that the checks carried out on February 8, 9 and 10,

2019 on a mobile phone with Android version 8.1.0:

On February 8, 2019, the Google Play Store is accessed, the LA app is located

LIGA – Official Football App and proceed to its installation: (…)

The app is executed, verifying that when starting it for the first time the

legal conditions of use. Next, the user is asked to accept the

processing of your geopositioning data and use of the microphone for the

detection of fraud in the consumption of football in public establishments, together with

other permits, which are found without premarking. Permissions are marked, accepting:

(…)

Next, a pop-up window is displayed asking if it is allowed

to LaLiga to record audio. Allowed.

It is verified that the app has a menu called "subscription center"

which, among other facilities, allows you to cancel permits. By means of it, the

permissions to use the microphone and the location for the purpose of fraud, and

checks, through the operating system, that the corresponding permissions are

are deactivated: (...)

It is verified that in the subscription center you can access the information of

the legal conditions: (...)

The app is uninstalled and reinstalled. It is verified that the same ones do not appear

screens than the first time the app was installed but if the permissions option

microphone and location for the purpose of fraud. This time it is denied

permission and it is verified that this permission is found in the subscription center

disabled. It is also verified through the operating system of the terminal that, in

the device configuration menu, in the application configuration it states that

permissions (micro and location) have not been granted for the app: (...)

On February 9, 2019, the app is reinstalled, executed and permissions are granted

of microphone and location for the purpose of fraud: (...)

Verifying that there is a match (Atlético de Madrid – Real Madrid) broadcast by BeIN

LaLiga and LaLiga TV, at 4:15 p.m., the application is accessed at that time: (...)

Looking at the mobile screen at various times, no icon is found

indicating recording activation or location. (…)

Yes, icons with the La Liga logo can be seen, consisting of advertisements for

notifications of goals or events in the matches:

There is also a symbol that looks like a data update, which is displayed

periodically about every 10 seconds in the center of the screen, and that

quickly disappears. Made a video capture for the extraction of a

frame with the image of this icon, shown below: (...)

It is accessed at the time the great game of the week is broadcast (Athlétic Club – FC

Barcelona), not meeting, looking at the mobile screen at various times,

no icon indicating recording activation or location.

b) The one provided in the allegations of LALIGA was incorporated as documentary evidence

c) The documentation was incorporated as documentary evidence on 02/20/2019

obtained from the website www.laliga.es/lfp.cuentas-anuales related to the Report

of Audit, Annual Accounts and Management Report as of June 30, 2018,

in PDF format, with the file name ccaa-lfp-2017-2018.pdf.

d) On 03/26/2019, the procedures for access to the

website of www.laliga.es regarding the privacy policy and screenshots

screen of a mobile device with Android 6.0 operating system in relation to

the notification bar and the activation of the geolocation function.

SEVENTH: On 04/08/2019, the instructor issued a Resolution Proposal,

in the sense of:

a) That the director of the Spanish Data Protection Agency file

to the NATIONAL PROFESSIONAL FOOTBALL LEAGUE, with NIF G78069762 the

imputation of the commission of the infringement of article 7.3 RGPD, provided for in the

article 83.5 a) of the aforementioned RGPD.

b) That the director of the Spanish Agency for Data Protection imposes

the NATIONAL PROFESSIONAL FOOTBALL LEAGUE, with NIF G78069762, of

In accordance with the provisions of article 58.2 j) of the RGPD, a sanction for the

commission of an infringement of article 5.1 a) of the RGPD, provided for in article

83.5 a) of the aforementioned RGPD, consisting of an administrative fine, in the amount of

500,000 euros (five hundred thousand euros) in accordance with the provisions of article

83. 1, 2 and 5 of the RGPD.

c) That the director of the Spanish Data Protection Agency order the

the NATIONAL PROFESSIONAL FOOTBALL LEAGUE, with NIF G78069762, of

in accordance with the provisions of article 58.2 d) of the RGPD for the infringement of the

article 5.1 a) of the RGPD, provided for in article 83.5 a) of the aforementioned RGPD, which:

adapt to the principle of transparency the use of the application in the terms

indicated in this resolution, through mechanisms that reinforce the

knowledge by users of the activation of the functionalities of

microphone and location of the devices that install the application, in the

moment this occurs. All this must be done within the term

of one month.

EIGHTH: After accessing the file and requesting an extension of the term – which was granted

by the Instructor – LALIGA presented on 05/06/2019, the allegations against the

Resolution Proposal, in which, in summary, it stated the following:

First. Of the main most relevant factual elements of the procedure

sanctioning

A chronological description of the events is made, emphasizing

mainly in that the practice of the test that was carried out in the

procedure instruction.

Second. The purpose of the function and the context in which the action takes place.

(...) This section is developed in terms similar to those described in the

allegations made to the initial agreement and the appropriate referral is made (...)

Being the purpose of LALIGA's action a legitimate and

provided, it was decided to understand that it should not be based on the interest

legitimate that is admitted as a legitimizing title of the treatment, but that it was required

the express consent of the interested party on two occasions with information

reasonable, weighted, visible and that requires an express acceptance so that the

functionality of the App can be performed.

LALIGA's actions are diligent, proactive and guarantee the protection of the

rights of citizens and should not be treated as if it were a breach

material was treated. The scope of the transparency obligation is being debated here

and the information that must be provided to the interested parties for their adequate

compliance.

At the time of the events, there was no evidence whatsoever that would allow us to know the

change of interpretation of the administration and therefore acted with diligence

that was required of him. With the motion for a resolution there is a change of level

requirement in relation to compliance with the principle of transparency.

Third. Regarding the determination of the amount of the sanction in the initial agreement and the

proposed resolution and its impact on the rights of LALIGA in the present

process.

The motion for a resolution not only fails to take into account the amount of the

sanction that could supposedly correspond for violation of article 5.1

a) of the RGPD, but proposes the imposition of a sanction that multiplies by

2.5 the amount of that.

The fact that the initial agreement establishes a sanction that "could

correspond" and then increase in the motion for a resolution deserves

certain considerations. The content of the initiation agreement with a

determination of the amount, with assessment of guilt and illegality

exceeds the content of the aforementioned agreement provided for by Royal Decree Law of 5/2018

and the LOPDGDD, in their respective articles 12.1 and 68.1. exceeds the mere

indication of the sanction that could correspond when making a determination

of guilt, with an assessment of mitigating and aggravating circumstances, without

by LALIGA nothing has been manifested. All this produces an absolute

defenseless, since at no time was he able to make use of his right to

power to reveal the inaccuracy of the assessment carried out by the body

sanctioning party to determine a limine the amount of the sanction that "could

correspond for violation of article 5.1 a) of the RGPD".

To which we must add that the initial agreement is dictated by the body

competent to resolve, making substantially the scope of action of the

competent body for the investigation, which could suppose a rupture of the

principle of separation between the phase of investigation and sanction, as indicated

the art. 63.1 LPACAP.

It is not ignored that the initial agreement may be related to the provisions of the

art. 85 of the LPACAP, however, in the case in which we find ourselves,

beyond the mere indication of a pecuniary amount, which would be applicable

in cases of a fixed fine, so that it only corresponds to the

charged to debate the effective concurrence of the typical assumption. In this case,

neither is the amount fixed, nor does it have to be pecuniary, however,

in the initial agreement the type of sanction and the amount have been specified without

LALIGA has been able to claim anything in this regard.

This quantification made in the Start Agreement is conditioning the

final decision that can be adopted as far as the amount is concerned, since

is marking the limit of the sanctioning reproach that can be imposed in the

process. A development contrary to what has happened in the present case,

where the very processing of the file has become a situation of

aggravation of the defendant's situation as a result of the mere exercise

of the right of defence.

In this case, the fact that the defendant does not renounce

the processing of the sanctioning file. Thus, when changing to

rise, or more correctly indicating in peius, the sanctioning reproach, it would be

admitting that the processing of the procedure can be punished by the

administrative body.

It has not been possible to demonstrate effectively during the investigation phase that

there are additional elements not taken into account in the initial agreement. The

investigation has not generated documents or evidence or elements of conviction

different from those that were taken into account in the initial agreement. Therefore, the

maximum amount of the sanction that could be imposed should not in any case

exceed the amount that he decided to include as a "sanction that could

correspond for violation of article 5.1 a) of the RGPD", incurring said

body, otherwise in a violation of the principle of legal certainty and

of the right to defense of this Part, by establishing a modification in peius

of the amount of the penalty.

Quarter. On the defenselessness in the processing of the file as a result of

tests practiced outside the procedure and the rules that regulate the test.

The provisions of art. 78 LPACAP, to the extent that it has been

practiced a test without communication to the interested parties, and therefore without their

presence, thus depriving him of the possibility of explaining some issues that

they were decisive. Producing helplessness, and to this end, it is convenient to bring

collation of the Judgment of 06/30/2011 of the TS, Contentious Chamber-

Administrative, Section 7.

In this case, tests have been carried out that have been incorporated into the

administrative file and that have probably been particularly

taken into account so that the sanction proposal rises from 200,000

euros to which the Start Agreement referred to the 500,000 euros proposed

be imposed by the Instructor, without at any time: (i) having been communicated

the practice of the test, (ii) the presence of LALIGA has been allowed in the

practice of the test, (iii) the presence of its technicians has been allowed to

to assist him and so that they could contribute to the formulation of allegations

complementary.

The presence of LALIGA in the practice of the test would have allowed to highlight

manifest the obvious errors in its practice, as discussed below.

Located in this plane could either cancel the practice of the test with all

its effects, or, bring the file back to the time of commission of the offense

procedural and practice the test under the conditions determined by law. And in

the procedural moment in which we find ourselves, it is difficult to articulate the

second option.

The tests carried out and incorporated without notification and on which the

disproportionate reclassification of the proposed sanction between the agreement of

beginning and the resolution proposal, cannot produce any effect because in the

present case there has been an effective defenselessness insofar as said

test has been decisive, as stated in STC no. 14/1999 of February 22.

The test referred to should not be taken into consideration

in the resolution issued. This test is actually the only activity of

instruction of the procedure so it is reasonable to consider that the same

has founded the modification carried out to graduate the guilt of

LALIGA, thus becoming a totally decisive test in this file.

Therefore, any increase in the amount based on said evidence – which

is the only additional evidence existing in the investigation phase (without

prejudice to the error in which it has incurred, which will be analyzed later)

would be infected with said vices of nullity.

Fifth. On the probative value of the inspection diligence incorporated into the file

without the knowledge of LALIGA.

Notwithstanding the nullity indicated, the diligence in folios 263 to 271

part of a completely wrong premise, and incomplete. First of all, the

The fact of having granted consent for the activation of the

microphone and geolocation functionalities do not automatically imply your

use. In the practiced diligence no icon appears simply because the

device used is not one of those selected by the LALIGA system of

all 50,000 sample users, and therefore is not one of the devices to which

which was accessed through the microphone and audio.

Second, the error is that it is assumed that the only

The privacy policy accessible to users is the one that appears in

the website of LALIGA as can be deduced from the diligence carried out in the

folios 351 to 361.

On folio 266 referring to the diligence carried out on February 8, 9 and 10

2016, the legal conditions of use of the app are shown and that they incorporate

a full first layer of your privacy policy, with links to

“Terms and Conditions of Use” and “Privacy Policy of the app” (page 4

of the diligence), without in said diligence contracting what was the content

of both documents at the time the investigation was carried out.

inspection. Assuming that said privacy policy was in the

same terms as in the procedure that occurred on June 21, 2018.

If these links had been accessed, it would have been known that the

privacy policy is not hosted on the website www.laliga./aviso-

legal-privacy-cookies referred to in the procedure of March 26, 2019,

otherwise

www.laliga.es/aviso-legal-privacidad-

cookies/oficial#androidprivacidad, being so that the information contained in

this last website further reinforces the guarantees of the principle of

transparency.

On 09/13/2018, a new privacy policy was developed and implemented.

privacy specifically referred to users of Android devices. (I know

attached as doc. No. 2 accreditation referring to the date of implementation of

the aforementioned privacy policy).

And in the new privacy policy (attached as doc. No. 3) it is specified in

more detailed terms than those required by art. 13 of the GDPR, the

treatments carried out. Including not only the information required by the

art. 11 of the LOPDGDD for the second layer, but additional information about,

for example, of the logic of the treatment in case of consenting to the use of the

microphone.

In the section on “purposes and basis of legitimacy for the treatment of

personal data”, stated the following:

Web

place

to the

C/ Jorge Juan 6

28001 - Madrid

http://www.aepd.es

https://sedeaepd.gob.es

25/85

(…) The additional purposes for which LaLiga

will treat your Personal Data, as well as the legal basis that legitimizes the

treatment for each of them (...):

ii. To detect fraud in the consumption of football in public establishments not

authorized. In case you have accepted the specific and optional box

enabled for this purpose, you consent to the access and use of the functionalities of

microphone and geopositioning of your telephone so that LaLiga knows from

which locations football is consumed and, therefore, to detect behaviors
fraudulent activities of unauthorized establishments related to the consumption of
football product. The activation of both the microphone and the
geopositioning of your mobile device, will require prior acceptance of the
Pop-up window that is displayed when you download the APP.
By activating the microphone functionality, the User is informed that
LaLiga may only capture encoded audio fragments or “fingerprints”
for the sole purpose of identifying the broadcast of an official match organized by
LaLiga, with the APP being able to access information through the microphone
only during the time slots of matches in which teams compete
of the league. Captured audio snippets are encoded on the phone itself
automatically through an algorithm that does not allow the process to be reversed,
in such a way that, once the sound capture made by the
microphone, said information becomes anonymized information being
its reversal impossible. Also, if you do not check the box enabled to
this, the user is informed that LaLiga may at no time treat
such information for this purpose.
The legal basis for the treatment of your data for the aforementioned purposes
mentioned is article 6.1.a) of the General Regulations for the Protection of
Data: the interested party gave their consent for the processing of their data
for one or more specific purposes. Your personal data will be
kept for these purposes until you revoke your
consent.
You have the right to withdraw your consent at any time in accordance with the
procedure described in the "User Rights" section, without this
affects the legality of the treatment based on consent prior to

his withdrawal.

In addition, a second section referring to "technical measures

specific measures implemented to protect the privacy of the user", where

describes the characteristics of the treatment, the moments in which it

may take place and even the technique used, which excludes conservation, and

including the collection, at no time of sounds, but only of the

their encoded fingerprint.

(…) LaLiga has implemented appropriate specific technical measures to protect

the privacy of the user if you enable the purpose of detecting consumer fraud

of soccer. These measures are detailed below:

Measures related to the use of the microphone:

- LaLiga will only activate the microphone of your mobile device during the periods

schedules of matches in which LaLiga teams compete.

- LaLiga does not access the audio fragments captured by the microphone of the

device, since these are automatically converted into fragments of

encoded audio or "fingerprints" on the device itself. LaLiga only accesses

anonymized information, which is irreversible and does not allow obtaining the information again.

audio recording.

- If this code coincides with a previous control code, LaLiga will be able to know

who is watching a certain match. If it doesn't match, the code is removed.

- We will periodically remind you that LaLiga can activate the microphone and

You will be asked to confirm your consent.

- To revoke their consent at any time, the user must

access the Subscription Center found in the APP menu or

either access the "Settings" tab of your mobile device and disable the

"Microphone" option.

The evidence on which the proposal has based most of its

argumentation suffers from defects that prevent it from being used as a means

decisive. Any assessment of a privacy policy other than the

relating to the application itself should be removed from the resolution ending

to the procedure. All of the above leads to the inescapable erroneous conclusion

who has had the motion for a resolution.

Sixth. About the scope of the treatment carried out by the LALIGA application.

The proposed resolution does not deny that the user has been informed about the

treatment of your data, but considers that the information is not enough for the

effects of the principle of transparency, art. 5.1 a) GDPR based on two issues

fundamental:

-the information in the first layer is not sufficient to guarantee the aforementioned principle and

-the right of the interested parties to be informed must be reinforced, since it is not

sufficient information provided at the time of initial data collection, it is

say, at the time the installation and first use of the application is carried out, but

that the information must be reiterated and carried out at each specific moment in

that the collection of any of the data occurs.

Such statements can be refuted because they do not respond to the reality of the treatment

carried out by the application, as can be easily contrasted through the Report

Expert opinion carried out by the Carlos III University of Madrid and by the undersigned.

(accompanied as doc. No. 4) which states, in summary, the following:

(i) The laliga application does not process personal data that

described in the motion for a resolution, since it does not deal with, collect or

stores the sound surrounding the user's terminal.

(ii) The only treatment of the user's IP address is the one carried out by the

balancer of the cloud computing service contracted to host the

information related to the application and the sole purposes of allowing the

interconnection between the user's device and the servers, without

store the aforementioned IP address in them.

(iii)

The only data linked to a person, as soon as it is

to single him out, which is not identifiable, is the random identifier assigned by the

service provider (THE COMPANY 1) of the LIGA (hereinafter FZID), in the

moment in which the installation of the application in the terminal of the

Username. For this reason, the treatment carried out by LALIGA is not only not

particularly intrusive, but implies the adoption of reinforced guarantees

of active responsibility in the sense provided in Chapter IV of the RGPD.

Seventh. Regarding the expert opinion issued at the request of LALIGA in relation to the

operation of the application and the processing of data by it.

The statements about the treatment carried out by the resolution proposal are

They do about three performances:

(YO)

The initial installation of the app on the device,

(II)

The inspection carried out on June 21, 2018; Y

(III)

The diligence carried out, without the knowledge of this party, on the 8th, 9th and

February 10, 2019, referred to in the sixth background of the proposal,

together with the reproduction of the privacy policy published on the website of the

league.

The affirmations, lacking evidential support, are (...) if there is treatment of

non-anonymized information, because what the microphone captures is the sound that is

happens in its field of action (which will depend on the quality of the model and

other environmental circumstances) may contain personal information

and third parties. And stopping at this first stage, there is no doubt that

produces a treatment, which includes, among other actions, the collection, registration,

organization, structuring. This possibility of collecting personal data

personal is what makes this treatment, tributary of the fulfillment of the

transparency principle. (…)

It is also stated that the treatment of the IP address and the

user identifier, assimilating it to other possible identifiers,

when I reiterate in the allegations that the user identifier (FZID) in the

treatment was different from any other identifier used for purposes of

commercial promotion or Google user ID. ?.

In particular, the report clearly indicates that the identifier attributed to the user

by the app does not allow identification.

It also notes the only information stored in the user's terminal, which

does not include in any case, the ambient sound.

It also shows how the soundtrack collection function is

programmed in such a way that it neither collects nor registers nor organizes identifiable sounds

surrounding the terminal. Thus it is noted:

“Thus, although the APP code would have the ability to save the

sound captured from the microphone, the APP's own programming prevents

this can be done. (...) thus it can be seen, in the highlighted portion,

how to create and save a file with that information for later

process it. However, in this case that code is disabled: in

this programming language, every line of code that is between the

flags /* and */ become non-executable”

As for the only treatment actually carried out, that is, the trace of

sound concludes that the fingerprint generation process, from the audio

original, is a transformation process that can be considered, with a very high

confidence level, as irreversible.

It also analyzes the way in which the activation or deactivation of the

access to the microphone of the user's terminal, concluding that (...) it can be affirmed

that the data collection function of the microphone is activated during the broadcast of

each match (…) for a maximum of 2 hours from the start of each match.

(…) the microphone data collected by the app has a duration of 5 seconds,

that are collected from activated devices every minute and if detected in the

environment the broadcast of LALIGA matches, or every 15 minutes otherwise”

And as for the possibility of reversing the fingerprint in a specific conversation,

concludes that “the design decisions of the fraud control mechanism prevent

that LALIGA can know the content of any conversation or identify the

potential speakers.”

The presumption of veracity and correctness that the procedural regulations surround the

action of the public administration, must go bankrupt since, the report is provided

expert opinion that must be considered as a sufficient evidence principle to unnerve

said presumption of veracity of the records of the Data Inspection. That is, the

presumption of veracity has been contradicted by the report provided.

Eighth. Consequences derived from the expert report described in the previous allegation.

The treatment does not respond to those described in the proposed resolution, nor does LALIGA,

nor THE COMPANY 1, store or use in any way the IP address assigned to the

device on your internet connection during football matches. The

IP is used by the balancer of the cloud computing service provider to

allow communication between the user's device and the server to which the information is sent.

information, without carrying out any treatment other than allowing the

bidirectional communication of information between the equipment and the server. It is neither captured nor

is not registered or stored in the app.

The only information stored on the servers will be that referring to the FZID that is

randomly assigned to each user of the app. So the LEAGUE is prevented from

reversal of the procedure, so that it will not be possible from the mere data of the FZID

of the user to know the IP associated with it and, even to a lesser extent, any other data

that allows you to make it identifiable.

The sound footprint and geolocation is only associated with the FZID, which in

no case will allow a later identification of the user.

Therefore, there is no information subject to treatment that can be considered data

of a personal nature in accordance with the provisions of article 4.1 RGPD and Co. 26 RGPD.

Neither LALIGA nor COMPANY 1 have at their disposal means that allow the

identification of the specific user of the app to which a sound print refers or

geolocation, for which the aforementioned Co. 60 must apply, which excludes from the application

of the RGPD those anonymous data.

Even when denying that data processing is not considered subject to

anonymization, it would not be possible to be before personal data, but in the worst case

we would be dealing with pseudonymized data, provided for in the RGPD article.

Despite the foregoing, and in application of the privacy principles from the

design, and in order to fully guarantee the rights of the interested parties,

a series of measures that are essential in this case:

-The consent of the users would be collected, to protect the treatment in the

art. 6.1 A) GDPR.

- users are informed in a clear and simple way, not of all the ends of the

art. 13 RGPD, but even the way in which the treatment would be carried out and the

logic of this.

-and as indicated in the privacy policy, users would be periodically reminded

users of the app that it will be able to proceed to the activation of the microphone and the

geolocation during the matches, giving them the possibility of confirming their

consent.

Therefore, it is accredited with the expert opinion provided that LALIGA does not process data that

directly or indirectly identify users of the app.

Ninth. Regarding the moment in which LALIGA must inform to guarantee the

compliance with the principle of transparency.

The instructor's proposal does not deny that information be provided to

users, but it is done insufficiently, so it understands that it must be notified

each time access to the microphone and geolocation of the terminal is activated. Front

to which the following should be indicated:

-no rule of internal law and of the EU imposes the obligation to inform

to the affected person at each specific moment in which a treatment of

your data.

-the user is not left defenseless in the face of alleged ignorance or possible

“forgotten” about the treatment, given that he has sufficient means at his disposal,

provided not only by LALIGA, but also by the operating system of the

device, to know the permissions granted.

Co. 39 determines (...) For natural persons it must be totally clear

that data is being collected, used, consulted or otherwise processed

data concerning them, as well as the extent to which said data is or will be

treated. (...) (the emphasis is from LALIGA). As can be seen, the diction of the

recital differs from the content in the proposal, since the present tense,

actually employed in it does not refer in any case to each moment in

that the treatment occurs, but to the fact of the treatment, to which it is effectively

refers to art. 13.1 RGPD, although limiting said reference to the moment of obtaining

the data. the RGPD refers to the interested party having knowledge when the

treatment is started, but in no case does it indicate that this knowledge should be reiterated

at each time such processing takes place.

It is not possible to interpret that when the RGPD establishes that the interested party must

be informed at the time of collecting your data, this obligation must

be fulfilled at each moment in which a collection of your data is carried out.

Which would lead us to interpret that, for example, in the case of a cookie,

It would be necessary not only the informative legend at the time of installation, but also

Every time the user would access a specific web page, they should be informed of

all the treatments that imply a modification contained in the cookies that

had on the device. This reasoning, unreasonable as it may seem

example, is but a consequence of the extrapolation of the reasoning contained in the

motion for a resolution, ignoring this part because I reason what would not apply to

profiling or tracking activities, such as the cookie, if it would be for the alleged

raised in this proceeding.

It is convenient to bring up Document WP260 rev01, of the Working Group of the

art. 29 on transparency, which the proposal itself cites, and taking into account that the

treatment cycle begins at the moment in which the interested party consents that by the

app you can access the microphone and geolocation functionalities of the

mobile device. , it can be concluded that said document does not impose on the person responsible

no type of additional obligation of information subsequent to that which occurs in

the beginning of the data processing cycle, is only imposed when appropriate

notice a modification of the information already provided. What is not produced in this

course controversial.

The proposal cites Co. 60 in support of its theses, and seems to conclude that the

reference made to the additional information is not of a qualitative nature, but

temporary in that each treatment must be reported. However, that

interpretation is not adjusted neither to the tenor of the RGPD nor to the interpretation that the

Same does Document WP260 rev01, cited above.

In addition, the information through icons as indicated in the proposal is

subject to the establishment of a prior standardization procedure, as indicated by the

art. 12.8 of the RGPD, which attributes to the European Commission the power to adopt acts

delegates for these purposes.

In conclusion, there is no rule of law of the union, nor right

Spanish that imposes on LALIGA the obligation to inform the interested parties about the

treatment of your data at each moment in which it is going to take place. But

This information must be given at the beginning of the treatment cycle.

Also, regarding the "temporary uncertainty" indicated in the proposal, between

the installation of the app, the provision of consent and the use of the microphone, and that

bases the obligation to inform in the required terms, would lead to establishing a

differentiation between the ways of informing, depending on the proximity to a meeting

determined, which is obviously impossible from a technical point of view.

Tenth. Regarding compliance by LALIGA with the requirements of the RGPD and LOPDGDD in

related to the principle of transparency. Information by levels or layers.

The appropriate reference is made to art. 13 RGPD, to Document WP260 rev 01, to the

The AEPD's own Guide for compliance with the duty to inform, to art. 11 LOPDGDD,

to conclude that apart from the provisions contained in the aforementioned elements, neither the RGPD, nor the LOPDGDD impose any additional obligation of information, linked or not to each specific collection of data that could be carried out in the future.

The privacy policy accessible from the application itself, and that was not taken into account by the AEPD in the inspection procedure on the 8th, 9th, and 10th of February 2019, as access to it did not occur on the occasion of said diligence.

In the diligence, the information accessible to the user of the app is reproduced in the first layer, which are referred to the general conditions, in terms of protection of data and whose reading is necessary to be able to continue with the process of using the enlargement and only once these conditions have been read and “following” them, requests the user's consent under the conditions provided for in art. 4.11 GDPR.

These legal conditions mentioned, contain a link to the policy of privacy of the application, accessible at the address www.laliga.es/aviso-legal-privacidad-cookies/oficial#androidprivacidad, accessible from the initial notice of legal conditions of the application, and incorporates all the information required in the second layer.

In addition to said information, the measures adopted in relation to with the use of the microphone and geolocation, specifically:

-access to these functionalities will only take place during the time slots in which LALIGA teams compete.

-you do not access audio fragments captured by the microphone, but the fingerprint Sound,

-You can revoke the consent in the subscription center that is

found in the application menu.

-that the application will periodically remind you of the fact that you can

access these functionalities, so that the interested party can confirm the

consent previously given.

In short, the art. 13 RGPD and 11 LOPDGDD through the

means recognized as suitable in Document WP206 rev01.

Eleventh. On the bankruptcy of the principle of legal certainty.

The social alarm indicated in the proposal must refer only to the

presentation of five claims related to the revocation of consent that

they were served.

The assessment of the existence of an infringement is based on considerations that are not

are taken into account by the European or Spanish legislator, given that the duty to

reporting must be carried out at the beginning of the treatment cycle, as required by

the criteria of the EDPB.

It is also indicated that it is not possible, from the information offered by the application,

know when the treatment will take place. However, it is specified that the

treatment will occur at times coinciding with the holding of meetings

that the LALIGA clubs celebrate.

The proposal refers to the fact that the treatment does not take place in the

moment in which the consent was given, concluding that “it cannot be the same, nor

subject to the same formalities, the consent given at a given time to

that a person in charge collects certain data and only those data, that the

consent given so that the person in charge can at any time, collect

data that by their very nature are changing or dynamic,” which leads to

conclude that “the principle of transparency demands a reminder, mark or signal that

said consent was given and that the treatment is taking place”

Well, there is no provision in the regulations that requires that the mode of

fulfilling the duty of information differs depending on whether there is a single collection of data or

several successive Therefore, the control authority could, before two assumptions of

treatments in which similar information is provided, decide that in some it would be considered

fulfilled the principle of transparency, while in another the principle would claim the

"reinforced" compliance with the duty of information, in terms that are not foreseen

in no provision and that they be established in each case based on what

the control authority considers appropriate.

Such a conclusion must be considered contrary to the principle of security

legal, guaranteed by article 9.3 of the CE. It is not possible for the Supervisor, in the

framework of some actions can modify the interpretation of the legislator, on the basis

of some considerations not foreseen by the legislator,

Finally, indicate that the considerations made by the proposal are wrong, for

how much:

(i) LALIGA has adopted numerous measures of active responsibility and

application of the principles of privacy by design in order to guarantee

that the treatments suppose a minimum interference in the rights and

user freedoms:

-no sound is collected, but an acoustic trace that is impossible to revert to

Audio.

-the treatment of the IP address does not take place, only the fingerprint is treated

audio and geolocation linked to an identifier, FIZD, which is not

can link to an identifiable person.

(ii) the information is that required by the regulations and also describes the

logic of the treatment to be carried out.

(iii)

LALIGA will periodically remind the interested parties of the

characteristics of the treatment and request the renewal of your consent.

And for geolocation, contrary to what is indicated in the proposal, the

location access icon, without the need to perform any type of

screen scrolling. This was demonstrated in the pouf document provided in the

allegations made to the initial agreement, where there was an attached video,

that shows such a condition at minute 1:55 to which the appropriate reference is made.

Twelfth. On the mitigating and aggravating circumstances referred to in the

resolution proposal.

The allegations made in the initial agreement in this area are reiterated, and

considers making a number of additional claims:

Of the measures adopted to alleviate the possible damages or losses

a)

derived from the treatment and the absence of negligence.

If measures were taken in this regard, they were also adopted after the

start of the procedure another series of measures aimed at reinforcing the principle of

transparency. As it was, that the processing of data that allows

an identification of the users, who may be considered anonymous, and

in the most rigorous of assumptions, pseudonymized. It was resolved not to treat the data of

the IP address for the purposes of fraud prevention and not to collect any sound

picked up by the device's microphone, nor on the servers.

Privacy from design is also accredited through the Expert Opinion

approved and demonstrates the principle of minimization.

All the considerations made in the report of the law firm are

taken into account, except for the display of an icon referring to access to the

microphone, since the capture of sounds does not take place, but a trace of

sound.

The geolocation icon is displayed.

Also, all of these averages were taken before the features came back on.

be activated after the start of the 2018/2019 season, in order to fully guarantee the

user rights:

The content of the information provided in the first layer was modified, which is

essential reading to continue.

Changed the text of the consent clause.

A new specific privacy policy was developed related to the

treatment, including non-mandatory terms in art. 13 GDPR for older

transparency, such as the logic of the treatment.

A reminder process was established about the possibility of access to these

functionalities.

The possibility for the user to revoke consent was established, not only

from the phone's own operating system, but with an additional procedure.

b)

Of the volume of affected subjects.

The motion for a resolution confuses the universe of users with what is simply

a sample of them. The number of 50,000 has not been increased, but

remains constant and is also static. Activation occurs only and

exclusively with respect to the same 50,000 terminals, not varying in the celebration

of each match.

The number of users is 4,227,848 users, it affects 1.2% of the users who have been

downloaded the application, even if all of them have given their consent.

c)

The non-existence of infringing conduct on the part of LALIGA.

The accreditation of compliance with said regulations up to the present moment can

be taken into account when establishing the amount of the sanction, notwithstanding that

“normal” is not to breach, as the proposal understands.

d)

From the collaboration with the AEPD.

Once the information regarding the application has been published, and in the event of a warning

related to the possible investigation of the facts carried out on the networks

(not addressed to LALIGA), was placed at the disposal of the control authority. The

argumentation of the proposal regarding the existence of a duty to collaborate would lead to the

interpretation that the mitigating factor provided for in art. 83.2 f)

GDPR.

and)

Of the alleged seriousness of the infraction.

The violation, which is denied, would only affect the fact that it has not been reinforced

To the extent that the AEPD considers the aforementioned information necessary to reinforce the

transparency principle. That is, it is not imputed that there is no information to comply

the principle of transparency, but deserves an addition.

LALIGA concludes requesting:

The annulment of the tests carried out ex officio.

The procedure file.

Subsidiarily, the conversion of the sanction into a warning.

Subsidiarily to the foregoing, the reduction of the sanction, without exceeding in any

case of the one established in the agreement to initiate the procedure.

The expert opinion is deemed to have been provided in accordance with art. 53.1 LCAP, and

the ratification of the report is offered in accordance with art. 335 and concordant

the LECiv,

Provisions relating to business secrecy are met.

NINETH. - Of the actions carried out, the following have been accredited

PROVEN FACTS

ONE. - On 06/08/2018 new functionalities of the LALIGA app were launched

referred to capturing audio and geolocation through mobile devices

that have the aforementioned application installed.

TWO. – On 06/15/2018 and February 8, 9 and 10, 2019, the installation of the

appLALIGA on a mobile device and once the application is installed in the section

GENERAL CONDITIONS OF USE AND PRIVACY POLICY appear in the section

3. USE OF THE MICROPHONE indicating the following:

(...) only in the event that you accept the box enabled for this purpose, as well as through the

pop-up window that appears in the APP, LaLiga will be able to activate the microphone of your

device to know if you are watching football matches. (…)

And section 4. USE OF GEOPOSITIONING, which indicates the following:

(...) only in the event that you accept the box enabled for this purpose, as well as through the

pop-up window that appears in the APP, LaLiga will be able to know your location through

of the geopositioning of your mobile device (...).

Both clauses indicate that the purpose is (...) to detect fraud in establishments

unauthorized public (…).

THREE. - Likewise, there is a link to which the information contained in the policy is sent.

of privacy of the web, regarding the moment in which the microphone is activated, is the

following (...) at times when competition matches are being played

football organized by LaLiga (...)

In the link hosted at https://www.laliga.es/lfp it is indicated that (...) It is an association

made up of all sports corporations and football clubs in

First and Second Division that participate in official professional competitions of

National scope (…)

FOUR. – The information referenced in the previous proven facts remains

in identical terms as of 03/26/2019.

FIVE. - On 06/15/2018 an installation test is carried out and it is verified that,

At the time of installation of the LALIGA app, pop-up screens of the

operating system requesting permission to record audio and access the location of the

telephone. Once in the application, no icon is seen (not found) on the

application that shows the activation of the microphone or the location, or icons or marks

that reflect the authorization for its possible activation. No information found

about the status of these activations within the options and menus of the

app.

SIX. - Regarding the operation of the LALIGA app in relation to the purpose of

detect fraud in unauthorized public establishments, the entity stated

during the inspection actions, among other issues, the following:

(…)This new functionality for fraud detection is enabled in the

appLALIGA since last Friday, June 8, 2018, only for system users

Android version 6.0 for its specific management of permissions) or higher and at the

national. This functionality uses pickups from the mobile device's microphone and the

location of this (...)

(…) There are about 10 million users of the LALIGA app. However, it has

enabled a limit of 50,000 users nationwide (only for Spain), number

maximum number of installations with this new functionality, which they estimate is enough to

sample for the intended purpose. Outside of Spain this functionality is prevented. (…)

In order for the microphone and location data to be processed for the stated purpose, the

The user must give their consent expressly accepting said treatments,

checking the box enabled for this purpose after reading the Conditions

General Terms of Use and Privacy Policy.

Yes, the IP address of the device and a

Specific identifier assigned by the LALIGA app to the user (Installation identifier

of the LALIGA app).

The user agent whose content depends on the manufacturer, and which

usually includes the version of the operating system.

either

Only if you decide to accept, the microphone will pick up binary codes of fragments of

audio, with the sole purpose of being able to know if the user is watching football matches of

competitions played by LaLiga teams, but the content will never be accessed

of the recording.

The location of the device is also recorded for comparison with the location of

catering establishments.

C/ Jorge Juan 6

28001 - Madrid

http://www.aepd.es

https://sedeaepd.gob.es

37/85

(...) With this procedure it can be ensured that no person or user, nor of LA

LIGA nor external to the entity, can access the sound recordings made by the

microphones, but only to some alphanumeric codes -the fingerprint-, since the

audios are transformed into the user's own mobile device (...)

(...) The reception of the location is done on a computer server of THE COMPANY

1, receiving by https (encryption) the latitude and longitude (location) as well as a mark

of time, the user identifier assigned by the LALIGA app and the IP address of the

device. (…)

(...) Since the location does not include the height parameter, it cannot be determined if

the user is in a bar on the street or in a private address or home

located at any height in the same vertical of the establishment. (…)

SEVEN.-. - At the time of execution of the device's microphone functionality

that involves capturing audio, no icon, mark or signal has been found, which

indicate that the microphone is being used. The entity under investigation as of 01/24/2019, has stated that it will not include any brand, sign or icon in this regard.

EIGHT. - At the time of execution of the functionality of the geolocation of the device supposed to access the location, a geolocation icon is displayed.

NINE. - In the inspection carried out, the entity stated, among other issues, the following (...) To capture the data (microphone and location) it is not necessary that the LALIGA app is running in the foreground, with computer processes running in the background (background) on the mobile device that allow the data collection. (…)

TEN. - Through the fraud detection process carried out through the LALIGA app, from the moment the information is captured, passing through the transformation, and shipment to COMPANY 1 and subsequent reception, is subjected to treatment, at least the following information: the audio that is picked up through the microphone, the IP address, a user identifier, operating system and device model, date and time and Location.

ELEVEN.- It appears in the documentation obtained in the previous inspection actions, an external report to the entity, carried out prior to the start-up of the new functionalities, where the following is recommended: (...) the establishment of restrictions on the use of the functionality, limiting temporary spaces and previously informing the user; display prompts or warnings to remind you of frequent way to the user that the sensors are collecting their personal data; Include in the application a specific icon by which the user can know in what moments LA LIGA collects audio and location.(…)

TWELVE: Contained in the documentation obtained in the previous inspection actions, information that reflects the internal meetings in LA LIGA of Privacy by Designa on the AppLALIGA, maintained in March 2018. (In this documentation it is recommended

anonymize the data obtained in such a way that it cannot be associated with any data

personal or identifier. Specifically, it is recommended not to process or collect identifiers

such as IMEI, MAC address, device id, advertising ID, serial number of the

device or IP address).

THIRTEEN: During the inspection carried out, it was revealed that the application did not

had a process for revoking the permissions to use the functionalities

referred to the microphone and location. Facing opposition rights, or facing a

revocation of consent, the entity referred to the configuration of the operating system

on the device to disable permissions.

FOURTEEN: On February 8, 9 and 10, 2019, it was verified that the LALIGA app

has a procedure enabled to disable the use of the microphone and the

Location.

FOUNDATIONS OF LAW

1. Competition.

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

control authority, and as established in arts. 47 and 48.1 of the LOPDPGDD, the

Director of the Spanish Data Protection Agency is competent to resolve

this procedure.

2. Previous Considerations.

Prior to the analysis of the applicable substantive law, it must be indicated

Regarding the allegations made by LALIGA (the entity investigated in the

successive) referring both to the lack of legitimacy of FACUA, and to the legal basis that

legitimizes the treatment that is carried out from the application (hereinafter the app), which the

This procedure is initiated ex officio, so it is irrelevant for the purposes

sought by the entity denounced, any pronouncement on the legitimacy

of that, and regarding the legal basis that legitimizes the treatment from the app, you must

It should be noted that these aspects are not analyzed in this proceeding, but rather the

compliance with the principle of transparency, so it is unnecessary to assess the

allegations of the investigated entity in this regard.

3. About the practice of the test and its challenge.

The investigated entity formulates allegations to the resolution proposal,

indicated with respect to the test practiced that there has been a violation of the

provided in article 78 sections 1 and 2 of Law 39/2015 of October 1, (LPACAP

hereinafter), which literally states the following:

1. The Administration will communicate to the interested parties, sufficiently in advance, the

start of the necessary actions to carry out the tests that have been

admitted.

2. The notification shall state the place, date and time in which the

proof, with the warning, where appropriate, that the interested party may appoint technicians

to be assisted

Based on this alleged violation, it understands that by not being notified,

has made him defenseless, an error of fact was incurred at the time of its practice, and that

had he been present at it, the result would have been different, being fundamental

annul the result of the same, because in addition to being the only test practiced in

investigation phase, its result is the one that supports the increase in the amount of the sanction

which was initially included in the initial agreement.

Against such statements, the following should be indicated:

The non-presence in practice of said test consisting of the installation of the

application on a mobile device and on the screenshot of what was displayed on the

itself, in no way can it be considered that defenselessness occurs, nor

violation of the guarantees of the alleged infringer as set out in

continuation:

As the investigated entity indicates, the principles of criminal law are

applicable with certain nuances to the sanctioning administrative law, since both are

fields of law, a manifestation of the ius puniendi of public power, and on the

basis of this application, it is interesting to analyze the principle of contradiction that is deduced

that the entity understands violated.

The Constitutional Court has advocated that the presumption of innocence

enshrined in article 24.2 of the Spanish Constitution (CE hereinafter) requires that

in the practice of evidence, the accused is assured of the possibility of contradiction.

(SSTC 74/2004 of April 22, 131/2003, of June 30 and 76/1990 of April 26 (...) the

exercise of ius puniendi in its various manifestations is conditioned by the

article 24.2 of the Constitution to the game of evidence and a contradictory procedure

in which their own positions can be defended (...)

For its part, the STC 56/1998 of March 16, indicates that (...) the values that

underlying the fundamental rights at stake – the presumption of innocence – require

to the evidence proceedings in the administrative order - sanctioning - are minimal

objective and subjective conditions that make its reliability possible. And if the first

seem to focus on (...) the possibility of contradiction (...) the latter allude to the

characteristics of the subject who practices them (...).

Implicitly the art. 78 LPACP recognizes the right of the accused to witness the

practice of evidence, but it is not a precept designed to inspire all means of

evidence, -since it makes no sense for documentary evidence, reports with

probative value, the written expert opinions - nor has the jurisprudence declared that those who do

are within its scope.

There are only two conflicting lines of jurisprudence regarding the

confrontations or testimonials, a minority jurisprudence that is in favor of the

presence of the accused (STC 07/31/2003; STS 07/15/2000),

and the majority jurisprudence for which the presence and

participation of the accused in the practice of the evidence, but, to guarantee the

contradictory principle, it suffices that it is subsequently granted the possibility of

examine the result that has been obtained and to allege in this regard what in his opinion

right suits. For this line of jurisprudence it is not necessary, therefore, the

immediate contradiction:

- STC 56/1998 of March 16, on testimonial evidence;

- STC 3/1999 of January 25, on testimonial evidence, where the court puts the

I emphasize that the accused (...) certain testimonial evidence was made behind his back,

with which he was deprived of an immediate contradiction, it is also true that this

irregularity did not cause the accused a deprivation of the necessary means for his

defense, because the testimonies were documented in the file (...) and the

plaintiff (...) had the opportunity to urge what was convenient on such evidence (...),.

- STS July 21, 2008 appeal 5469/2004, - on the inspection

ocular in audita part-

- STS of March 18, 2004, on testimonial evidence.

- STS of May 21, 2008, on the reports issued ex officio and without

intervention of the accused: they respect the principle of contradiction if later they are

transferred to make the appropriate allegations.

In the present case, the contested evidence practiced in audita parte, consists

in downloading the application on a mobile device, and incorporation into the file

of the information displayed on the screen of this, through a document, a

diligence. It makes no sense to ensure the presence and intervention of the accused in his

realization to guarantee the contradiction through its intervention in it.

In this case, the contradiction is guaranteed by providing the accused with a copy

of the document that collects the result of said practice. In this sense it is appropriate

bring up the STS of June 9, 2003 (rec. 8463/1998) – where the accused,

is also LALIGA, and deals with the admission that the contradictory principle in the

reports with probative value provided by the Administration is satisfied in the phase of

pleadings or hearing.

He alleged – as in the present case – the violation of the principle

contradictory, since the Competition Court admitted that in an IMA report it was

incorporated into the file “with secrecy” since “those denounced were not notified and

has had a relevant influence on the sanctioning resolution” according to the sentence (…) the

reason must be dismissed (...) because such report (...) was available to the

denounced in the hearing phase before the Competition Court and were able to allege

contradictorily.

On the other hand, the Constitutional Court has repeatedly declared (for all, Judgment 14/1999, of February 22) that the materiality of defenselessness “requires a relevant and definitive deprivation of the powers of allegation, proof and contradiction that unbalance the position of the accused”, indicating the Supreme Court in its Judgment of November 16, 2006 (Rec. 1860/2004) that “for there to be defenselessness determinant of the annulability of the act, it is necessary that the affected party has been unable to adduce in support of their interests how many reasons of fact and of law may deem pertinent to it”.

From the foregoing, in no way can it be seen that it produced any type of defenselessness to LALIGA for not having been present in the practice of the test, since his result has been revealed to him and he has formulated the allegations that he has

had to good, fruit of which the present valuation is carried out.

Notwithstanding the foregoing, -and assuming that the proposed sanction, contrary to what LALIGA indicates, is not based solely on the result of the practice of said test, -it must be considered that its result has to be reconsidered with regard to the display of an icon on the device screen, only for activation of geolocation, namely:

In the documentary evidence provided in the allegations made to the agreement of beginning, the entity stated that a video was included showing the icon of the geolocation, to which the instructor did not have access when he indicated that in the support presented by LALIGA, - a pen drive memory - only found

documents in PDF format, and none in video format. However, just as

alleged LALIGA and as has been verified later – the video was attached to the

document in PDF format related to a navigation record, being able to check what

claimed by the entity.

In the same sense, in the test carried out referring to the installation of the

application on February 8, 9 and 10, 2019 (folios 263 to 271) includes the

result that can be summed up in that no icon is found with respect to the

geolocation – or the microphone.

It should be noted that this test is requested ex officio by the instructor, on the

basis that the delivered external memory -pen drive – did not contain the file in format

of video, (which, as already indicated in the previous paragraph, did contain it).

Faced with the result of this, LALIGA explains that the reason why it does not appear

the aforementioned icon is because the device where the test has been carried out is not one of the

that LALIGA selects within the sample of 50,000 users.

For the above, taking into account the factual error in the practice of the test

by the instructor, and the allegations made by LALIGA regarding the

result of the evidence carried out on folios 263 to 271, it must be concluded that the

The application shows an icon related to the activation of geolocation when it is activated.

active, as stated in proven fact eight.

4. On the request for “expert” evidence, its effects and other references to the

extension privacy policy.

In the allegations made to the proposed resolution, LALIGA provides a

report-opinion of "experts" that collects considerations regarding the operation

of the application, and requests that said opinion be included in the list of evidence of the

procedure and if the instructor deems it necessary, the presence of the

authors of the report for ratification.

The right to proof is a right of legal configuration (among many

SSTC 131/2003, 96/200; 174/2008) which has various consequences, and in what here

it is intended to assert, in terms of time and form on its proposal.

The jurisprudence affirms that any proposition of proof that is not carried out

in the manner and at the time provided by the applicable regulations may be rejected

by informal or extemporaneous. Thus, for example, it is convenient to cite the STC 131/2003 of 13

June, which declares that (...) since it is a legal configuration right, it is

It is necessary that the test has been requested in the legally established manner and at the time

(…)

The proposition of evidence is preclusive in the procedure

administrative sanction, so that, after the moment of making it, the proposal will be

extemporaneous and its lawful dismissal for which it would not violate the fundamental right

former art. 24 CE. (This is affirmed by STC 131/2003 of June 30 and specifically by the SSTSJ of

Andalusia, considers the request for evidence time-barred when formulating allegations to the

motion for a resolution, as intended by LALIGA)

In the present case, in the Agreement to initiate the procedure, it is when

opens the term to "formulate allegations and to propose evidence". Therefore, it is not possible

admit for the purposes intended by LALIGA, the expert opinion provided together with the

allegations made to the proposed resolution or require the presence of the

authors of the opinion for its ratification.

However, to the extent that the report is incorporated into the allegations of the

entity, expressly citing paragraphs thereof, may be, -to that same extent,

object of analysis and contestation.

Secondly, on the factual elements that are accompanied in the

processing of allegations made to the resolution proposal, it is indicated with respect to the

privacy policy referred to the application, which, in the test diligence practiced

by the instructor on February 8, 9 and 10, 2019 in folios 263 to 271, no

the internet link relating to the application's Terms of Use was accessed, and that

had they accessed, the information hosted on www.laliga.es/aviso-

legal-privacy-cookies/official#androidprivacy that already existed since 09/26/2018,

collected a specific privacy policy of the application.

In view of this, it must be pointed out that in the proceedings on folios 351 to

361, dated 03/26/2019, contains the privacy policy to which the

navigation when clicking on the link established for this purpose in the Subscription Center of the

application, which seems illogical then, that on that date there is a policy of

specific privacy for the application in the link that is cited by LALIGA in its

allegations, and that, in turn, there is another in the Subscription Center established at

effect for the app. That is to say, assuming what LALIGA stated for the purposes of

purely dialectical, there were two privacy policies depending on whether you accessed

from the link hosted in the application when accepting the conditions or if it was accessed from

the Subscription Center or from the web (as is still the case on the date of

05/16/2019)

To which must be added, that it is surprising that, if indeed it existed at

that date said privacy policy of the application (09/26/2018), will not be provided in

the allegations made to the initial agreement that occur on the date of 01/24/2019.

In conclusion, there are doubts regarding the date on which the

produces the modification of the privacy policy, which the entity has not achieved

clearly establish, there is only the certainty that said privacy policy

exists at least since 05/05/2019, which is the date of its capture and printing,

that accompanies the arguments made to the motion for a resolution.

Therefore, the effects intended by LALIGA regarding the policy of

privacy, in this procedure they will take effect a posteriori, that is, from the

05/05/2019, validating the assessments in this regard that are made in the Proposal

Resolution of the Instructor.

Thirdly and lastly, regarding the list of evidence for the proposal for

resolution, LALIGA maintains that the only evidentiary element carried out in the

instruction that supports the increase in the amount of the sanction initially planned is

precisely the diligence of evidence that requests to cancel.

Against this, it should be noted that it was incorporated as documentary evidence,

In addition to the result of the previous inspection actions, the allegations

formulated to the initial agreement, which is where LALIGA states that it has not included (or

it follows that he is going to do it) some icon regarding the use of the microphone.

And it is these terms and their consequences (temporary and quantitative) that

support said increase in the sanctioning reproach and not so much that in the aforementioned

due diligence it is indicated that the geolocation icon is not shown, when

indeed it does show up.

5. On the concept of personal data processing and the concept of data

staff.

Article 4.1 of the RGPD determines the concept of personal data,

establishing that it considers as such (...) all information about a natural person

identified or identifiable ("the interested party"); shall be considered an identifiable natural person

any person whose identity can be determined, directly or indirectly, in particular

by means of an identifier, such as a name, an identification number,

location data, an online identifier or one or more elements of the

physical, physiological, genetic, mental, economic, cultural or social identity of said

person(…).

Article 4.2 of the RGPD determines the concept of treatment, which considers

as such any operation or set of operations performed on data

personal information or sets of personal data, whether by automated procedures or

no, such as the collection, registration, organization, structuring, conservation, adaptation or

modification, extraction, consultation, use, communication by transmission, diffusion or

any other form of authorization of access, collation or interconnection, limitation,

deletion or destruction;

The investigated entity alleges regarding the existence of personal data and its

treatment, that personal data is not processed, that there is no treatment

itself and therefore is not subject to the duties of information and

transparency that are estimated by the AEPD to be insufficient or deficient in the agreement of

beginning, and which are confirmed in the proposed resolution of this procedure.

Specifically, it indicates that to the extent that the information obtained through the

microphone becomes a fingerprint on the device using the application, without

be audible, does not constitute information in the strict sense that allows it to be attributed

condition, among which is information concerning personal data

but, at most, it could be pseudonymized data in accordance with the

art. 4.5 GDPR.

In support of this statement, LALIGA provides an Expert Report (the Report in

hereinafter), and that without prejudice to the form and time of incorporation into the

procedure, which cause it to be treated as information annexed to the allegations, must

indicate that, it could "verify" the circumstances of the application from the date of its

performance from now on, that is, from 05/05/2019, and it must be remembered that the

The moment that this procedure analyzes is from June 8, 2018, until

minus the formulation of allegations to the initial agreement (01/24/2019) where

acknowledges that no icon is displayed or will be displayed regarding the use of the

microphone, which converts the imputed conduct into a continuing infraction.

Based on the foregoing, LALIGA's allegations focus, in summary, on the

circumstance that there is no processing of personal data, (i) or in terms of audio

which is accessed through the microphone, (ii) nor in terms of information regarding the

IP address and the identifier that is sent to the servers of THE COMPANY 1.

As a starting point, it is convenient to analyze the mechanism of operation of the

application regarding the use of the microphone and geolocation functionalities,

along with other information aggregated in the context of its fight against fraud in the

broadcasting of football matches, taking into account the manifestations of LALIGA,

both in the on-site inspection carried out, and in his allegations made, both at the

initiation of the sanctioning procedure and after the resolution proposal.

In short, it can be said that the user gives consent for the

application access the information captured by the microphone, and after its transformation in the

own device into an acoustic fingerprint or fingerprint, this along with other information

is sent to the servers of the person in charge of the treatment - THE COMPANY 1 - for the purposes

to compare said set of information, with the acoustic footprint of the emission of a

soccer game, so that if they coincide - if there is a match - the location of the

device and it can be verified, with the information offered by the geolocation, if the

The user's device is located in an establishment that broadcasts the games of

LALIGA with the corresponding license.

From the foregoing, it can be concluded that, in all this information processing,

there are at least three clearly defined phases or temporal stages: (i) the collection or

collection of information, (ii) its processing or transformation and finally its (iii)

its shipment and collation.

5.1 About the information accessed through the microphone:

The designed system used by the application inevitably requires the

Capturing ambient audio is a fundamental part, without which it would not work.

In that audio, there is no doubt that character data may be contained

personal, own and third parties, simply when a conversation is captured.

Although the report provided establishes that audio is not accessed by the

LALIGA, also reiterates on numerous occasions that what is captured is the information

that is obtained through the microphone, that is, the sound.

The user has given his consent so that LALIGA can treat the

information obtained through the microphone, so that, in the first stage of the set

of the process, it can be stated that if the uptake occurs during a conversation

where personal data is indicated, we will be facing a capture or collection

of personal data and, therefore, before a treatment of personal data.

In the proposed resolution of the instructor it was indicated that as a result of the

allegations made to the initial agreement where the existence of treatment was denied

of data, the following (...) Against this, it must be indicated that, if there is treatment of

non-anonymized information, because what the microphone captures is the sound that is

happens in its field of action (which will depend on the quality of the model and other

environmental circumstances) may contain own personal information and

third parties. And stopping at this first stage, there is no doubt that a

treatment, which includes, among other actions, the collection, registration, organization,

structuring. This possibility of collecting personal data is what makes

this treatment, tax compliance with the principle of transparency.

A different question is that, subsequently, and that is what the entity affirms

investigated, the sound is converted into a fingerprint, which is what is

sends to the servers of THE COMPANY 1, for comparison. Well, in this second

This stage is when another phase of the treatment of “data

personal” captured by the microphone, which includes adaptation or modification,

extraction, consultation, use, communication by transmission, diffusion or any other

form of authorization of access, collation or interconnection, limitation, suppression or

destruction. Or to put it another way, the process of conversion into a fingerprint constitutes

in itself one of the phases of the global treatment, which begins to take place from the

collection of the information, regardless of the subsequent processing, and finally the

sending or communication for comparison.(...)

As can be seen, the concept of treatment encompasses the collection or

data collection, without prejudice to subsequent processes. In this case, there is no doubt

that the sound is collected, which may contain personal data, so it is

necessitates the brand being claimed. (…)

The entity states, both in the allegations made to the initial agreement

such as those made to the Motion for a Resolution, that the audio is not stored in the

device and that it is in this one where the transformation in the fingerprint takes place,

almost immediate way.

It is worth citing as an example, what is related to storage is indicated in the

allegations where an excerpt from the report provided is included indicating that (...)

“Thus, although the APP code would have the ability to save the sound in a file

captured from the microphone, the APP's own programming prevents this from being able to

carried out. (...) so you can see, in the highlighted portion, how it was created and

I kept a file with that information to later process it. Nevertheless,

in this case that code is disabled(...).

The report provided by the entity whose extracts are included in the

allegations made to the motion for a resolution, offer an explanation of the

operation of the application that must be understood to reflect the conditions to be

date of May 6, 2019 (and not from June 8, 2018 to that date), and

also that explain an element of great importance, we are facing a process whose

configuration obeys the will of LALIGA (like any person responsible for a

computer environment), but the accent should be placed on relevant issues such as the (i)

existence or not of storage, (ii) the moments of activation of the microphone, (iii) the

rigorous fingerprint creation procedure (including when and how long takes time to occur and its irreversibility), (iv) the set of information that is sent to the servers of AMAZON - referred to quantitative and qualitative aspects - and (v) the consequences that can be extracted from the whole process, in the sense of giving compliance with the fight against fraud in the broadcast of soccer matches for which a specific device has been identified that is obviously carried by a user.

The user grants consent so that LALIGA can process the information accessed through the microphone- The process that will happen on the device, when LALIGA agrees, is that the operating system will receive a "request for access" to the microphone by the application, and that will grant it, that is, it will allow that the application obtains the audio that picks up the microphone of the device.

And this is where we must first stop, to determine the existence of the need for the supplementary information in terms of transparency claimed in this resolution.

That, at a later time, the processing of the captured audio takes place, and that it is done in one way or another, depends solely on the will of LALIGA, because as can be deduced from the report itself, the computer environment is easily modifiable by changing the programming with the determination of some values or others. -second phase of treatment-.

On the ease and willingness to modify the values, in addition to the affirmation that has been collected from the Report provided, serves to show that when it has LALIGA has seen fit, has identified a specific mobile device, by provide the navigation record of a "selected" terminal from the sample of 50,000 users, to display the image displayed on the screen for evidentiary purposes pretended. That is, by modifying some "values" in the programming of the software, proceeded to identify the device whose "navigation" it intended to display.

In short, that consent granted to use the information, and the

possibilities offered by computer environments with respect to their configuration, together with

other elements that will be revealed throughout this resolution,

make the icon, mark or signal demandable that they are using said

information.

Therefore, in the first phase of the treatment, in capturing the audio,

obtains information from the user's device, which may contain data of a personal nature

staff.

5.2 About the sending of information and its collation. The existence of character data

staff.

On folio 35 of the file, which refers to the Inspection Act of the month

of June 2018, it is recognized by LALIGA that the IP address of the

user's device, along with the user identifier that the application assigns.

(also on folio 76).

The entity stated in its allegations of 01/24/2019 made to the agreement of

beginning on page 228 that:

(…) the IP address of the device and the user agent were used for the purposes

exclusive of having a complementary control layer with the purpose of

guarantee (as far as technically possible) two limitations: a) only activated

on devices in Spain, which is deduced from the IP and, b) they were only activated on

devices with Android versions greater than 6.0 which is deduced from the user

agent(...) thus adding an extra control filter(...), It should be noted that the user

agent was not linked to any personal data of the user beyond the IP address

and location, which was necessary to be able to pair it with the device and ensure

that the permissions granted by the user to the app were applied.

Processing of the device's IP address and user agent was discontinued.

The specific identifier that the application assigns to the device allows to relate

the data obtained, without being linked to a specific user.

(...) In order to reinforce the principle of transparency, when development

allowed, both the IP of the device and the user agent were no longer treated, without prejudice to

that this would suppose an extra loss of control of verification of the scope of the

treatment. (…)

That is, it is admitted that the IP address of the user's device was treated, but

does not indicate the specific moment regarding when it was stopped being used – only

LALIGA offers explanations in the allegations made to the resolution proposal

on the date of 05/06/2019 of how the IP address is treated, as later

analyze.

To which we must add that at least until the date of 03/26/20191, it is reported

in the privacy policy hosted on the web page that is collected from the user the

IP address and a user identifier is assigned, indicating that "the codes will not be

referred to your name, but to your IP address and the specific ID assigned to you by the APP

when you register (folio 352). (The underlining is from the Spanish Agency for the Protection of

Data).

Even as of 05/16/2019, this statement is maintained in

https://www.laliga.es/aviso-legal-privacidad-cookies/, that is, the IP address is processed

of the user's device (along with other information that is explained later).

In the Proposed Resolution of the Instructor, the following was stated:

1 Date that the indicated circumstances have and that were incorporated into the evidentiary element, notwithstanding that as

of the date

of 05/16/2019, information on the collection of the user's IP address continues at https://www.laliga.es/aviso-legal-

privacy-cookies/ when referring to the operation of the application.

C/ Jorge Juan 6

28001 - Madrid

http://www.aepd.es

https://sedeaepd.gob.es

48/85

(...)..in the actions carried out, it has become clear that, in the policy of

privacy of the entity's website, to which the application information is sent

indicates that the following personal data are processed:

(…) IP address, your operating system, your browser ID, your browsing activity

navigation and other information about how they interact with our LaLiga Environment.

We collect this information as part of log files, as well as

through the use of cookies or other tracking technologies. For this purpose you

We inform that we use the Android and IOS advertising identifier to analyze

ads and users and serve ads. This may be associated with information from

personal identification or other identifiers such as device identifiers

persistent (for example, SSAID, MAC address or IMEI), or to any new identifier

of advertising. (...).

In this sense, it should be noted that, in the privacy policy hosted on the

website of the entity, in section 3.5 Purpose of the treatment, expressly indicates that

(...) the codes will not refer to your name, but to your IP address and the specific ID

that the APP assigns you when you register (...) (folio 27).

Likewise, it was revealed in the inspection carried out on the date of

06/22/2018, (hereinafter the inspection) that underwent treatment the following

information when the microphone and geolocation functionality is activated in the

application: the fingerprint resulting from the conversion of the audio, the IP address of the

device, a specific identifier that the application assigns to the user, and the user

agent , and all this was transmitted, for comparison (to the servers of THE COMPANY 1)

with another fingerprint of the broadcast of a football match in real time.

On folio 76 there is an example of a "trace" after the comparison of

information coincided, including, among others, the date, the existence of a coincidence or

match, the IP address of the user's device, a user identifier, the

operating system and its version, and the device model(regarding the content of the

user agent, the entity stated in the inspection carried out that this information informs

which varies depending on the device being used, but is mainly used to

check the version of the operating system).

Likewise, on the same folio 76 there is an example of sending information referred to

to the geolocation, where together with the user identifier, the latitude and the

length.

All this information must be considered personal data, and its

processing, fits into the actions that in the definition of paragraph 2 of article 4

of the RGPD, are instituted in treatment.

(…)

First of all, it must be indicated that the IP address of the user's device and the

location, with the remaining associated information (folio 76) must be considered data of

personal character. And secondly, despite the fact that it is indicated that the

IP address and user agent, at least until the date of 03/26/2019 is reported in the

privacy policy hosted on the website that is collected from the user's address

IP and a user identifier is assigned, indicating that "the codes will not be

referred to your name, but to your IP address and the specific ID assigned to you by the APP

when you register (folio 352).

For not indicating that, in the application's Subscription Center, it happens that

when the use of microphone and geopositioning is authorized, it is indicated as

conditions of such use "included in the Privacy Policy of the App

Official of LaLiga", which, in turn, refers to the privacy policy of the website

(folio 268). That is, again the user is told the same thing as indicated in the paragraph

above and on page 352.

In short, the reported entity states that it does not undergo treatment

the IP address and the user agent of the device, and instead, not only that information appears

in the privacy policy of the app, but also in the Subscription Center,

that did not exist at the date of the on-site inspection actions, also

refers back to that information: to the capture and processing, of the

IP address and user ID.

Based on the foregoing, it has been proven that the app processes

User information that can be categorized as personal data

staff. Therefore, the person responsible for the application, the investigated entity, is instituted in

responsible for the treatment and therefore is subject to the obligations derived from the RGPD

and its sanctioning regime. (…)

5.2.1 Arguments made to the proposed resolution.

LALIGA declares regarding the information it sends to LA servers

COMPANY 1 (which has contracted with AMAZON for hosting "in the cloud"),

Next:

(ii) The only treatment of the user's IP address is the one carried out by the

balancer of the cloud computing service contracted to host the information

related to the application and the sole purposes of allowing the interconnection between the

device of the user and the servers, without storing in them the aforementioned

IP adress.

(iii)

The only data linked to a person, insofar as it makes them stand out,

which is not identifiable, it is the random identifier assigned by the service provider

(THE COMPANY 1) of the LEAGUE (hereinafter FZID), at the time the

installation of the application on the user's terminal.

And in the annex to the Report - of May 6, 2019 - that is provided together with the

The following is indicated regarding the treatment of the IP address:

(...) When a new request arrives at the balancer, it redirects the request and the

converted to internal network traffic, which is not public. Thereafter, the source IP

it will be that of the balancer, an internal IP, and only values will be reflected in the traces

internal. Throughout the processing from the HTTP balancer there is no access to the

IPs of origin, nor are they recorded or stored in any way (...)

In other words, LALIGA states that, regarding the sending and comparison phase of the

information, only the acoustic fingerprint and the FZID identifier are sent with a

IP address, no longer of the user, but of the "balancer". Of having for certain those affirmations, could take effect from your contribution to the procedure.

However, they contradict what was indicated by LALIGA both in the inspection carried out as in the allegations made to the initial agreement. In the first, regarding the use of the IP address of the user's device was accompanied by a trace of the information sent once the match or coincidence was verified (folio 76) where it was stated what following (...) an example trace after finding a match between fingerprints. The IP and the user agent allow to control a priori and a posteriori, the requirements: SPAIN, Android,>=6.0(...), and in the latter, indicate that the IP address used is that of the user's device, (...) with the aim of limiting the scope of the treatment and being able to audit, a posteriori, the operation of these controls, thus adding an extra filter of control (...) (folio 228).

By stating that "a posteriori" it is admitted that the IP address of the device of the user -and not of the load balancer- is the one that is object of treatment even after verifying the collation of the sent signals. This information is also add that of geolocation.

But, what is more, even with a date subsequent to the allegations made to the Resolution proposal (05/16/2019), on the entity's website, follows informing about the treatment of the IP address of the user's device.

So, as explained below, with all the information added,

We may be dealing with personal data processing.

5.2.2 On the "direct or indirect" identification of users.

At this point, we can affirm without a shadow of a doubt that the application collects at least the IP address of the user's device, the unique identifier that is assigned to the user's device by the application itself, the acoustic fingerprint and the geolocation.

All this information linked to a user can be considered personal data.

personal nature, as it is suitable for identifying users “directly or indirectly”.

The investigated entity maintains that there is no identification of the user,

but at most we are facing a singularization.

Faced with this, and admitting what was alleged for mere dialectic purposes, it must be indicated

that singularization is nothing but a modality of identification. With the information that

is sent, it is possible to create an unequivocal profile of a user and that it can be

objectively differentiate from another, that is, it can be isolated and extracted

information, differentiate it from another, and attribute some consequences, (without it being necessary

know terms referring, for example, to the name, surnames, email address, Nick or

registry aliases). What is relevant is the ability to distinguish this set of

information of another, for which, we have first made an identification, without which

we would not have comparative terms to be able to make such a distinction, and attribute

certain effects to it: in this case, determine if the user is in a local or

establishment where football matches of teams from the National League of

Professional soccer. and after the appropriate process, find out if said establishment issues the

I find the corresponding license.

This interpretation was already endorsed by the Art.29 Working Group in its Opinion

4/2007 “On the concept of personal data2” when analyzing the term “indirectly”

as a way to carry out the identification.

Specifically, it indicated the following: (...) when we speak of "indirectly"

identified or identifiable, we are referring in general to the phenomenon of "unique combinations", be they small or large. In cases where, At first glance, the available identifiers do not allow a person to be singled out determined, it can still be "identifiable", because that information combined with other data (whether the data controller is aware of them or no) will distinguish that person from others. This is where the Directive refers to “one or more specific elements, characteristic of their physical, physiological, psychological, economic, cultural or social. Some of those features are so unique that make it possible to identify a person effortlessly (the "current Prime Minister of Spain"), but a combination of details belonging to different categories (age, regional origin, etc.) can also be quite conclusive in some circumstances, especially if you have access to additional information of a certain Type. This phenomenon has been extensively studied by statisticians, always willing to avoid any breach of confidentiality.

At this point, it should be noted that while identification through name and surname is in practice the most common, this information may not be necessary in all cases to identify a person. so it can happen when other "identifiers" are used to single out someone. Indeed, the computerized files of personal data usually assign a unique identifier to the registered persons to avoid any confusion between two persons included in the file. On the Internet, too, traffic control tools make it possible to identify with ease the behavior of a machine and, therefore, that of the user who find behind. Thus, the different pieces that make up the personality come together. of the individual in order to attribute certain decisions to him. Without even requesting name and address of the person it is possible to include it in a category, on the basis of socioeconomic, psychological, philosophical or other criteria, and attribute

certain decisions since the individual's point of contact (a computer)

makes it unnecessary to know his identity in the strict sense. In other words, the

ability to identify a person is no longer necessarily equivalent to the ability to

be able to get to know their first and last names. (...) (emphasis is from the Agency

Spanish Data Protection)

2 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.

In short, and taking into account what is stated in the cited Opinion, with all the

aggregated information that the application processes, – and no matter how much the

report provided by the investigated entity makes categorical statements in the sense

contrary- we are faced with a treatment of personal data, which, together

with the exposed characteristics, is creditor of the informative complement in terms

of transparency that is demanded in the present procedure.

6. On the characteristics and context of the processing of personal data

analyzed and its relationship with the principle of transparency.

6.1 Normative determination.

It establishes article 5 of the RGPD under the heading “Principles related to the

Treatment”, in section 1 a) the following: 1. Personal data will be: a) processed

lawfully, loyally and transparently in relation to the interested party ("lawfulness, loyalty and

transparency"); (the underlining is from the Spanish Data Protection Agency).

The data processing that is carried out through the LALIGA application, in the

user devices, derived from the functionality of the microphone and geolocation,

violates the principle of transparency provided for in article 5.1 of the RGPD, as

exposed throughout this resolution. In support of this statement, one must turn to

the following items:

First of all, Recitals 39 and 60 of the RGPD determine the following:

(…) All processing of personal data must be lawful and fair. For natural persons

it must be absolutely clear that they are being collected, used, consulted or processed

otherwise personal data concerning them, as well as the extent to which such

data is or will be processed. (...) (The underlining is from the Spanish Protection Agency

of data).

And (…) The principles of fair and transparent processing require that the

interested party of the existence of the treatment operation and its purposes. The person in charge of

treatment must provide the interested party with as much additional information as necessary

to ensure fair and transparent processing, taking into account the circumstances and

. (...) (The underlining is from

the specific context in which the personal data is processed

the Spanish Data Protection Agency).

As can be seen, the text of Recital 39 uses verbs in their form

present, so that at the time they are being collected, used,

consulting or treating the information captured by the microphone and the geolocation, - that

obviously it does not happen when the application is installed and the treatments are accepted in

a first moment - that additional information is necessary, such as,

for example, a warning in the form of an icon or brand, which would allow the user to know that

treatment "in real time", which would serve to complement the information received

initially, given the specific context in which the information is processed (Co.

60).

6.2 Allegations to the proposed resolution.

LALIGA, in its arguments made to the motion for a resolution, focuses on

debate, fundamentally, in the temporal space with respect to which the

treatment, or as it indicates, “the cycle of treatment”. To justify that the information

must be offered in the different "layers" is the one provided for in art.13 RGPD and concordant

of the LOPDGDD – which understands that it satisfies amply-, and that the moment

temporary referred to in Recital 39 of the RGPD in relation to the obligation to

transparency, is when the treatment cycle begins, that is, when it is discharged

the application and the conditions are accepted.

Likewise, it proposes in comparative terms the requirements of information and

consent in the cases of Internet users referred to the download and

installation of data storage and retrieval devices (DARD in what

hereinafter or "cookies"), indicating that it is not required that, each time you access the

information that said devices collect, the user is informed.

As a starting point, it is necessary to analyze the moment in which the

data processing in the operating system designed by LALIGA in the

app. Bearing in mind the concept of treatment provided for in art. 4.2 GDPR –

transcribed ut supra- to check if it occurs or not, and when it occurs, interested in

At this time, highlight the use of expressions such as: (...) collection, registration, (...).

Considering the operation of the application as explained by LALIGA,

such arguments must be rejected outright. There are elements in the file

that clearly indicate that the treatment does not occur at that precise moment, it is

that is, when the download occurs and the acceptance of the conditions.

Precisely as LALIGA has explained throughout the procedure, the

audio information and further processing will occur during the moments of

“broadcasting of the matches of the LALIGA teams”. That is, the "material treatment" is

occurs during data collection, and at the time of download, installation of

the application and acceptance of its conditions, only the acceptance of the

conditions.

We are not dealing with "ordinary" data processing, where, for example, a

Internet user registers in a form on a website for a certain

purpose, where obviously at that precise moment the collection of their

data, and as LALIGA indicates, it is not logical and it is excessive, to report every time

make use of the data.

But, in the present case, the treatment occurs each time it is collected

microphone, the user's IP address, the online identifier given

of geolocation that does not have to be the

the information of the

assign by application

same, when the application is downloaded and the conditions are accepted.

and the

information

The concept of "treatment cycle" proposed by LALIGA in its pleadings

formulated to the motion for a resolution, if admitted, it would happen from the first

effective data collection, which obviously does not occur with the acceptance of the

conditions, since the application does not require a prior registration process for its use,

nor does it collect the audio when accepting the conditions, but when actually

the information you can obtain is useful for the purpose pursued.

Finally, indicate that regarding the comparison that LALIGA makes with the

information requirements in the use of DARD or cookies, the proposal made by the

investigated ignores a fundamental element, in that case the user does not harbor any

doubt that you are using the internet, that you are "browsing" with your terminal, and after the

information offered and consents granted, there is no doubt that it is fully

aware of the possibility that your navigation offers information that may be

used by the DARDs.

However, in the case of the LALIGA application, none of this occurs, given

that the affected party can carry their device, practically at all times, without being

making effective use of it, for example, you can carry it in your pocket, in the car,

etc., that is, in any act of the development of their private life that has nothing

to do with the use of the device. That is, "the expectation of privacy" cannot be the

same in one case as in the other. Since it is LALIGA – and not the user – who decides

when and on which devices the aforementioned functionalities must be activated.

Therefore, the arguments proposed by LALIGA in this regard must

be completely rejected.

6.3 Characteristics of the treatment.

Given the above, and in relation to the specific context and the characteristics

of the treatment that make him worthy of that adaptation and complementarity

informative, it should be made clear as a starting point, that the devices

Mobile phones (tablets and smartphones) are devices that are characterized by their multiple

functionalities, since they are widely used both as telephones, agendas,

cameras, as well as for Internet access. In addition, the possibility of installing

applications on these devices expands these functionalities practically without limit,

making it very difficult for the user to remember all the consents or permissions they have

granted in each of the installed applications, as well as their management.

Being mobile phones devices that their users are used to carrying

with them in a continuous and generalized way, the fact of the possible activation of the

microphone and the location of these devices can lead to situations of

alarm among users, who understand that they may be being watched at all

moment. This intensifies the need to provide them with additional information to

ensure transparent processing, which should include the scope of such processing

(how and when), and inform "in real time" that the microphone and the

geolocation.

In this sense, in the previous inspection actions (as stated in

sections 2.4.G and 5.1 of the second antecedent of this resolution, to which

timely referral is made) it was learned that the application is still

running and sending information, even if it is not running in the foreground.

sic. For data capture (microphone and location) it is not necessary for the

application is running in the foreground, there are computer processes

running in the background (background) on the mobile device that allow the

data collection.

Second, as stated before,

should be taken in

consideration that we are dealing with a treatment that does not occur immediately

after giving consent, but the collection of data, and the remaining

actions object of treatment can be carried out, with very high probability, in a

separate moment in time.

Namely, a user downloads the application and if, for example, he has just finished

a day of the national league championship (or any other competition organized

by LA LIGA according to the information they offer), it will not be until the next day (or

until the next competition organized) and during the broadcast of the football match

that the entity wishes, when the information will be collected and sent

(that is, the moment in which the treatment will materially take place)

That lapse between the acceptance of the functionalities described and the moment in which

which the treatment actually takes place (consisting of the collection of audio,

user's IP address, unique identifier and location and its subsequent submission and that

depends on the will of LALIGA and therefore it can happen at one time or another)

makes it necessary to adapt the principle of transparency to this type of processing,

being essential to inform with certainty and transparency about when

will produce the treatment - both at the time of installation of the application, and

during the collection of information -, in particular in the most intrusive ones such as the

capture of sounds by the microphone and geolocation.

LALIGA in its arguments made to the proposed resolution, indicates that

(...)Likewise, regarding the "temporary uncertainty" indicated in the proposal, between the

installation of the app, the provision of consent and the use of the microphone, and that it bases

the obligation to report in the required terms, would lead to establishing a

differentiation between the ways of informing, depending on the proximity to a meeting

determined, which is obviously impossible from a technical point of view.(...)

Against this, it should be noted that, precisely in order not to establish a differentiation

between the ways of informing and the multiple possibilities of different spaces

between the proportion of information regarding the use of the microphone and

geolocation and the true uptake, it is necessary to be informed in the

when the capture is taking place.

Therefore, it is convenient to carry out the analysis of the information provided in the

two clearly differentiated stages: the first, when consent is given

for the treatment and the second, in terms of the information provided to the

affected during the execution of the treatment itself.

7. Information provided at the time of application installation.

7.1 Checks during the instruction of the procedure.

According to the instruction carried out, it has been verified that, at the time of the

installation of the application, and therefore to grant the consent of the user of the

application, the following information is provided in the CONDITIONS section

GENERAL USE AND PRIVACY POLICY:

The existence of two texts is verified, one that after checking the box

corresponding the user accepts that (...) I have read and accept the legal conditions and the

privacy policy of the App (...) being a link to the website of the entity and a

second text that after checking the corresponding box the user accepts (...)“ Doing

By clicking here, you accept that LaLiga processes your personal data, including those obtained by

through the microphone of your mobile device and geopositioning, to detect

fraud in the consumption of football in unauthorized public establishments"; (folios 9-

10).

Once the application is installed in the GENERAL CONDITIONS OF

USE AND PRIVACY POLICY appear in section 3. USE OF THE MICROPHONE that

indicates the following:

(...) only in the event that you accept the box enabled for this purpose, as well as through the

pop-up window that appears in the APP, LaLiga will be able to activate the microphone of your

device to know if you are watching football matches. (…)

And section 4. USE OF GEOPOSITIONING, which indicates the following:

(...) only in the event that you accept the box enabled for this purpose, as well as through the

pop-up window that appears in the APP, LaLiga will be able to know your location through

of the geopositioning of your mobile device (...).

Both clauses indicate that the purpose is

(...) detect fraud in

unauthorized public establishments (…).

This is the only information that, at the date of the entrance exams

during the instruction of the procedure, it showed the application when installed and in the

moment of accepting the activation of these functionalities.

Moment that, as has been reiterated during this resolution, is far from

the time with respect to when, effectively, the microphone and the

geolocation.

And not as indicated by the denounced entity that states that it was already included in the

"legal conditions" of the app menu as of June 9, 2018, since the text that

contributes in its allegations to the initial agreement, in this respect it corresponds to the

privacy policy of the website and therefore it is not information that is offered

during the provision of consent. Worse still, admitting as true that

affirmation, neither can it be clearly deduced when the event will actually take place.

this type of treatment.

That is why this informative complement is claimed, taking into account the

characteristics of the treatment that is analyzed, to give full effectiveness to the principle of

transparency.

Even if the user accesses the website on 03/26/2019 (pages 27 and

351 and following), the information provided therein regarding the

application, referring to the moment in which the microphone is activated, is the following (...) in the

times when organized football matches are being played

by LaLiga (...) said information is excessively ambiguous since the user of the

application cannot know a priori, which are the competitions organized by the

entity, especially considering that we are dealing with an entity that is defined in

its website3 as (...) a sports association made up of all the societies

anonymous sports companies and First and Second Division soccer clubs that participate in

national professional official competitions.(...).

Which is a great difficulty, even makes it impossible for a normal user

can know without a shadow of a doubt when the functions described are being used and

when your personal information is being processed.

In short, when the tests described were carried out, it was not explained, with

the clarity and transparency required by a treatment as intrusive as the one that has been

described, when the information captured by the microphone and the location of the

device. Hence, informative complementarity is claimed.

The investigated entity alleges in its defense that including this information is not

required neither in article 13 of the RGPD nor in article 11.2 LOPDGDD, nor in the guides

published by the AEPD and therefore their implementation cannot be required.

Faced with this, it is necessary to make the appropriate reference to the Considerations of the

RGPD, indicated above and to the formulas proposed by the opinions of the Group

of Labor of article 29, which have been assumed by the European Committee for the Protection of

Data and that were indicated in the Initiation Agreement, since they answer questions about the

why the information claimed in this procedure must be included (i) for the

natural persons it must be made absolutely clear that they are being collected, used,

consulting or treating, for what purpose said complement should be introduced

informative (ii) the person in charge of the treatment must provide the interested party with

supplementary information is necessary to ensure fair treatment and

transparent, taking into account the specific circumstances and context in which

process personal data, and how it can be done (iii) Another possible way

of providing transparency information is through the use of “push” notices and

"pull". Push notices involve the provision of information notices of

ad hoc transparency, while “pull” notices facilitate access to information

through methods such as permission management, privacy dashboards, and

3 https://www.laliga.es/lfp

"learn more" tutorials. These allow for a more transparent experience

user-centric for the stakeholder.

7.2 Allegations to the proposed resolution.

In the arguments made to the motion for a resolution on the date of

05/06/2019, LALIGA indicates that:

There is a specific privacy policy of the application that is accessed

through the links "Terms and Conditions of Use and Privacy Policy of the app"

that was implemented from 09/13/2018, and several

internal emails.

Against this, it should be noted that as explained in FD4, there are elements

in the file that make question the true date of modification and

implementation, and even admitting for purely dialectical purposes the existence of this

the date indicated, the proceedings carried out would then show that

two different privacy policies would coexist, depending on where you access the

the same (informing in one that the IP address of the user's device is not treated and

in the other the opposite). Therefore, what there are no uncertainties about is that from the

date of 05/05/2019 there is said privacy policy, since the

checks for these purposes.

In the link www.laliga.es/aviso-legal-privacidad-cookies/ there are submenus, one

of them referred to the official application at www.laliga.es/aviso-legal-privacidad-

cookies/official that is the same one to which navigation is redirected when accessing

through the application, which adds the #androidprivacidad field to the URL, which is what

determines that the scroll of the page shows the precise information of users with

ANDROID devices.

Beforehand, it should be noted that, at present, the information hosted

At www.laliga.es/aviso-legal-privacidad-cookies/ there is information regarding the

application where it continues to state that the user's IP address is collected.

From the privacy policy hosted at www.laliga.es/aviso-legal-privacidad-cookies/official the following should be highlighted:

In case you have accepted the specific and optional box enabled for this purpose, you consent to access and use of the microphone features and geopositioning of your phone so that LaLiga knows from which locations consume football and therefore, to detect fraudulent behavior of establishments not authorizations related to the consumption of the football product. The activation of both microphone as well as the geopositioning of your mobile device, it will require prior acceptance of the pop-up window that is shown when you download the APP.

By activating the microphone functionality, the User is informed that LaLiga may only capture encoded audio fragments or “fingerprints” with the sole purpose of identifying the broadcast of an official match organized by LaLiga, the APP being able to access information through the microphone only during the

time slots of matches in which LaLiga teams compete. The fragments of Captured audio is automatically encoded on the phone itself using a algorithm that does not allow the process to be reversed, in such a way that, once the sound capture made by the microphone, said information is converted into anonymized information being impossible to revert

(…) Measures related to the use of the microphone:

- We will periodically remind you that LaLiga can activate the microphone and

will ask you to confirm your

consent. (

…)

(…) Measures related to the use of geolocation:

- LaLiga will only access your location during the match time slots in

those who compete in LaLiga teams.

- We will periodically remind you that LaLiga can access your location and

You will be asked to confirm your consent. (…)

From reading it, it can be deduced that it does not clearly explain the

operation of the application, as LALIGA has shown in the

present procedure. Indicates that “you can only capture fragments of audios

encrypted”, when the truth is that he first captures the audio and then, as he affirms,

encodes, as it is clearly observed one thing and the other are not the same.

The temporal uncertainty regarding access is maintained in identical terms

to the information collected through the microphone “during the time slots of matches

in which LaLiga teams compete”. Whether by the organization itself

national league championship, either due to the circumstance related to the election of the

specific matches in which it is decided to activate the control, the truth is that this uncertainty

can only be reduced with the display of a sign or icon, when

the information obtained through the microphone is actually being accessed

of the device, “in real time”.

And finally regarding the confirmation of the consents indicated in

the aforementioned policy, indicate that LALIGA, taking into account the time since they are used

the indicated functionalities 06/08/2018 has had the opportunity to allege and prove, the

existence of this and has contributed nothing in this regard, that although it does not replace the existence of

a mark in "real time", can limit that temporary space between the original

acceptance of the conditions and when the information obtained is actually used.

through the microphone.

In conclusion, the existence of an ad hoc application privacy policy

for Android OS version, it does not cover the gaps in terms of

transparency that are claimed for it, which makes unnecessary the icon that

is claimed. In other words, no matter how much the provisions of the

articles 13 RGPD and 11 LOPDGDD, the system itself designed by LALIGA that provides the

treatment of some special characteristics, will not prevent the need for

reminder, mark or signal that is claimed in this instance.

As a closing argument, indicate that LALIGA repeatedly cites, both

during the previous inspection actions, in the allegations to the agreement of initiation and

even in those made to the motion for a resolution, that the operation is similar

provided by the SHAZAM4 app - which picks up sound through the microphone and sends it

to a server for comparison- , ignoring a fundamental difference and that if it occurs in the

LALIGA application, this procedure would not make sense: in that application,

it is the user himself - and not the service provider - who decides to activate the

microphone for audio pickup to occur, be encoded, sent, and

collate, -if that circumstance were to occur, in the present case it would not be necessary to

icon sign-.

However, none of that happens here, but it is LALIGA who decides when

start the process and on which users, with prior information with the

uncertainties that have become apparent.

8. Information provided during the execution of the application.

From the practiced instruction it is deduced that the user is not informed, in the

time of activation of the use of the microphone from the start of the use of the application in

the month of June 2018 to the present.

8.1 Regarding the use of the microphone.

It is the investigated entity that openly admits in its allegations that it does not include

any type of information in that sense, indicating the following (...) after carrying out a

weighing judgment between the purposes of the treatment pursued and the rights and

freedoms of the interested parties, understands that the inclusion of an additional icon to the entire

information already provided would be excessive, it would not provide additional guarantees to the

protection of the rights and freedoms of the interested parties and would be invasive for the

users by including on their device elements and images that could be considered

annoying, hinder the use of the App and generate a false perception that it is being

recording the voice and the conversations that are taking place around the device,

giving rise to an unnecessary social alarm (...)

Faced with this, it is necessary to refer to what is already indicated in the Agreement to Start the

this procedure where in its section III.4 the following was indicated, (...) The

treatment that is carried out by the LALIGA app, requires an adaptation of the

principle of transparency, taking into account the special characteristics of which have been

indicated, the result of which is the adoption of measures that guarantee the full

knowledge of the user that the described functionalities have been activated and, therefore,

therefore, that the treatment in question is being produced or carried out. Is essential

that the method or methods chosen to provide the information are appropriate

for the specific circumstances, therefore, the quality, accessibility and understandability of

information is only as relevant as the actual content of the information on

transparency, which must be provided to stakeholders.

4 https://www.shazam.com/es

In this sense, it is especially illuminating, in relation to the case

analyzed, what is included in the document Opinion GT260, of November 29, 2017

regarding Guidelines on Transparency under Regulation 2016/679

elaborated by the Working Group of Article 29 –and ratified by the European Committee of

Data Protection-, indicates in its section 39 the following (...) Another possible way of

providing transparency information is through the use of “push” and “pull” notices.

Push notices involve the provision of ad transparency information notices.

hoc, while "pull" notices facilitate access to information through methods

such as permission management, privacy dashboards, and "more" tutorials.

information". These allow for a more user-focused transparency experience.

user for the interested party. (...) (The underlining is from the Spanish Protection Agency

of data).

It should also be noted that the aforementioned document in section 43 indicates what

following (…) Recital 78 refers to data controllers who

apply measures that meet data protection requirements by design and by

defect, including measures consisting of transparency with respect to the functions

and the processing of personal data (...) (The underlining is from the Spanish Agency for

Data Protection).

Finally, it should be noted that even the legal reports provided by

LALIGA (requested from two independent third parties for the analysis of adaptation to the

privacy and data protection regulations) referenced in section 5.2 of the

second antecedent of this initial agreement, expressly indicate as

safeguards to be taken into account, the establishment of restrictions on the use of the

functionality, delimiting temporary spaces and previously informing the user;

display notices or warnings to frequently remind the user that

sensors are collecting your personal data; Include an icon in the application

by which the user can know when LA LIGA collects audio and

Location.(…)

The investigated entity states in its allegations made to the settlement agreement

start that has made a weighing judgment and given the result or conclusion to which

has arrived, it is observed that it has not taken into account the criteria of the regulatory body,

that is clearly deduced from the beginning of this sanctioning procedure, nor the

opinions of the Article 29 Working Group indicated in the opening agreement, nor

the own reports of the entities that she herself has commissioned on the

safeguards to consider when using the microphone functionality of the

devices, mainly emphasizing the difficulty of use that the

addition of additional information, in addition to generating a false perception that

is recording the voice and conversations, ultimately indicating not wanting to generate

an unnecessary social alarm, all this in the face of compliance with the principle of

transparency in the processing of personal data collected by the RGPD.

Given these statements, it should be noted in the first place that the inclusion that

the microphone has been activated, or in other words, that it is capturing audio that is

occurs around the device, by means of a warning or icon, it would not generate a false perception that the voice and conversations are being recorded, because precisely that is what happens when the microphone is activated (the audio is captured and therefore both voice and conversations that are taking place), the perception that users would form, it would not be false at all, but very likely, and in second term, it should be remembered that as a "social alarm", it generated the first weeks of the month of June 2018, when jumping to the media the news that the app captured audio and without knowing how or for what purpose. Maintain the application in identical conditions that, on those dates, did not would correct that perception, but rather the opposite.

For this reason, the exercise of transparency demanded in this instance, far from increase this public perception of permanent scrutiny of privacy, would clear any doubt in this regard and would put in the hands of users the freedom to choose if they really grant their approval for the capture of the audio.

Be that as it may, in the present case subjective perceptions of one and the other (correct or infused), but the strict compliance with the RGPD and its principles, so the information gaps revealed, both when installing the application, as during the execution of the functionality, in addition to being corrected, must complete with the display of an icon or sign, so that the user knows that audio is being captured with your device, in accordance with article 5 of the RGPD and the interpretation made by Considering 60, and the opinion of the Working Group of the article 29 assumed in its entirety by the European Committee for Data Protection, all they partially transcribed ut supra.

In the allegations made to the proposed resolution, LALIGA reiterates

in the non-enforceability by any European or national standard, in the way in which it must be

report for the analyzed treatment, indicating that it amply complies with the provisions

in article 13 of the RGPD and 11 of the LOPDGDD. Against this, it should be noted that no

is analyzing the adequacy of the information offered regarding the precepts

indicated, since it is observed that they have been complied with, but that the type

of treatment with the notes of intrusiveness and temporal (and physical) uncertainty regarding

of the place where the user is), revealed, claim that

introduce elements that reinforce the principle of transparency.

In arguments made to the motion for a resolution, an attempt is made to explain the

moments of activation of the microphone, and therefore of data collection (...) the function

microphone data collection is activated during the broadcast of each game of

First Division, becoming active for a maximum of 2 hours from the

start of each match. In addition, the microphone data collected by the APP has

a duration of 5 seconds, which are collected from activated devices every minute if

the broadcast of LALIGA matches is detected in the environment, or every 15 minutes in case

contrary (...)

Taking this forecast into account, it cannot be concluded, as indicated by LALIGA,

that the display of an icon referring to the use of the microphone hinders or annoys the user

with excessive icons on the screen, given the length of time of its use.

In addition, precisely the sample of the same would nullify any alarm

relative to the fact that users may be permanently monitored, since

thus, they would know at what time and at what not, the information is being captured

via audio, so they could decide when to withdraw permission from the app

to access such information.

8.2 Regarding the use of geolocation.

In this regard, the entity states that (...) the operating system of the

device shows, by default, an icon in the notification bar at the time of

location capture (...) the notification bar is always visible,

as shown in the Agency's own Diligence dated June 15, which

work in the file, as well as in the video provided by this party to this document

of allegations as document No. 3. Both pieces of evidence reflect that, in the bar of

device notifications, visible at all times during activation of the

functionality of the app, a geopositioning icon is displayed which appears

punctually during the broadcast of the matches (...)

The Instructor's proposed resolution indicated in this regard what

following (...): In view of this, it should be noted, first of all, that in the proceeding

on folios 6 to 11, no such indication is shown. In document No. 3, relating to the Act of

the attached screenshot, no icon is displayed either

geolocation, and regarding the video file referred to, indicate that no

found on the USB stick attached to the pleadings, but simply

various documents in pdf format.

In this sense, and to verify the assertions of the investigated entity,

carried out tests on the dates of February 8, 9 and 10, 2019, in order to verify if there was

said information on the screen of the devices that use the application, whose

result works on folios 263 to 271, and the following were verified, among others:

ends:

(…) Verifying that there is a match (Atlético de Madrid – Real Madrid) broadcast

by BeIN LaLiga and LaLiga TV, at 4:15 p.m., the application is accessed at that time(…)

It is not found, looking at the mobile screen at various times, any

icon indicating recording activation or location.

Yes, icons with the La Liga logo can be seen, consisting of advertisements for

notifications of goals or events in the matches (...)

There is also a symbol that looks like a data update, which is

periodically displays approximately every 10 seconds in the center of the screen,

and it disappears quickly. Made a video capture for the extraction of

A frame with the image of this icon is shown below:

C/ Jorge Juan 6

28001 - Madrid

http://www.aepd.es

https://sedeaepd.gob.es

64/85

It is accessed at the time the great game of the week is broadcast (Athletic Club

– FC Barcelona), not meeting, observing at various times the screen of the

mobile, no icon that indicates activation of recording or location.(...)

In short, contrary to what was stated by the entity, no

no icon showing the activation of the geolocation function.

After the allegations made to the proposed resolution by LALIGA, it has been

verified that the PDF file was improperly accessed, and that if

contained the video of the navigation with the activation of the geolocation, and

Regarding the content of the evidence procedure, it was explained by LALIGA that the reason why

which did not show any information on the device where the tests were done,

it is because it was not one of those selected within the sample of 50,000 users.

For all these reasons, the allegations in this regard are upheld and it is concluded that

displays a mark, signal or icon, in real time, that the information is being accessed

geolocation. Circumstance that has been assessed when qualifying the appropriate sanction

impose and that modifies the meaning of the proposed resolution of the instructor in what

regarding the amount of the fine.

9. On compliance with the principle of transparency.

As has been indicated before, we are dealing with data processing that requires

special reinforcement of the principle of transparency and in view of the instruction carried out,

It follows that the entity has done nothing to effectively comply with the

regarding the use of the information accessed through the microphone of the

device.

The information that gives content to compliance with the principle of transparency

in this type of treatment it must be concrete and decisive; should not be formulated

abstract or ambivalent terms or give rise to different interpretations, such as

happens in the present case in relation to the type of data processing that is carried out

out through the app.

9.1 Characteristics of the analyzed system and lack of transparency.

The lack of information in terms of transparency: the information that is

provides the user of the application, both at the beginning - at the time of download,

installation and acceptance of the conditions - and above all during the execution of the

treatment (at that time it can be stated that there is no information), it is shown

insufficient in relation to the type of treatment that is carried out, in relation to,

(Yo)

(iii)

The temporary space produced between the moment in which the

consent – with the information that is provided that contains

uncertainties- and the one that actually produces the data collection.

The moments of activation of the aforementioned functionality. Considering the

information offered when accepting the conditions (either in the first layer or in

(iii)

second layer), referring to activation "in LALIGA team matches".

And the moments of activation of the aforementioned functionality when they can

occur in the development of the most exclusive areas of the user than anything

have to do with the initial object of the functionalities, which according to

LALIGA is limited to "protecting your team" (soccer team) and

“Detecting fraud in the consumption of football in public establishments is not

authorized”. Precisely because of the random element about when

will produce the activation -which does not depend on the user, nor does it have a priori elements

to know when it will occur-, and its relationship with the development of the

private life of the user, it is necessary that he knows in all

moment, when the device's microphone is being used. As

may take place without your knowledge in a strictly private or

family and collect personal information from someone who has given consent

with the characteristics pointed out, and from third parties, which are obviously unrelated to

the purposes pursued by LA LIGA.

In relation to the operation and effectiveness of the application with the

in order to prevent fraud, at the expense of user privacy,

that, if finally there is no coincidence between the compared codes

(the one that is sent from the device with which it is available on the servers

of the entity), it is something that only happens and can be verified a posteriori,

that is, when the processing of the data has already taken place, or even

having existed coincidence, it can occur with respect to the effectiveness of the

geolocation system, this may not fulfill its purpose because the

device may be at another altitude that the system is not capable of

discriminate. It may happen that the device is in a building with several

plants, capturing information in the private address of a third party, and that

associate the information processed with that of a place where it is not located. The

modifications introduced by the entity regarding the creation of “a

heat map” also does not solve the indicated random element. Definitely,

the treatment carried out may not serve the purpose intended by LALIGA and by

both occur outside of it with the expectation that it will work, with a

high cost for user privacy.

In short, the owner of the personal data being processed does not have

available a simple mechanism or provided by the person in charge that

let you know without any doubt that the LALIGA application is

accessing the information that is collected by the microphone of your device.

As the user has not been informed of the possibility of capturing in the second

flat.

Nor can the informative legend used with

character prior to marking the box for the provision of consent, since

it is not possible to interpret the temporal or physical space that can be

deprived of when the treatment is going to be executed, not even going to the policy

of privacy hosted on the main web page (nor at the date of the inspection carried out

or if you want at present folio 351 and following), nor even to the web page where

collects the specific privacy policy for users of Android operating systems

which is proven to exist as of 05/05/2019.

That is why this guarantee is necessary in favor of users, in terms of

transparency that is claimed in this sanctioning procedure.

9.2 Violation of the principle of transparency.

Therefore, it has been proven that the data processing that is carried out through

the LALIGA application, on user devices, derived from the functionality of the

microphone, violate the principle of transparency provided for in article 5.1 of the RGPD, in

relation to the special characteristics of this treatment, which can be summarized in

the following:

(i) Certain treatments take place, such as capturing audio,

geolocation, user IP address, unique identifier, fingerprint creation and sending

digital, at a time other than the expression of consent, and given the

characteristics of these treatments (information provided at the time of the

installation, means used, level of intrusiveness of these, temporary circumstances

risks of the user's private life, etc.,., all of them analyzed throughout the

this resolution) it is necessary a reminder, mark or signal that indicates without

no doubt to the user, they are actually taking place. well the

material treatment does not occur when a user downloads and installs the application –

where the conditions are accepted – but it will come later.

This reinforcement or reminder of the consent given at the time of

downloading the application is due to the circumstance that it cannot be the same, nor subject to the same formalities, the consent given at a given moment so that a responsible collects certain data and only those data, that the consent lent so that the person in charge can at any time, collect data that by their own nature are changing or dynamic, as for example happens with those of geolocation (it is very likely that the location will change with respect to the at the time consent is given, at the time the data is collected), that in themselves are not "a datum" but a category of data, being alien to this circumstance the affected party, in such a way that the principle of transparency demands a reminder, mark or signal that treatment is occurring at that precise moment in time and physical space that occurs when the mentioned functionalities.

(ii) It does not appear in the informative legend that is shown in the installation of the application on the mobile device, the specific moment in which the functionalities, nor can it be inferred from the privacy policy hosted on the main web page.

(iii) There is no icon or other signal indicating that the functions are being used. mentioned functionalities

(iv) there is a possibility that the application runs in the background and therefore both without the user's knowledge. (as stated in sections 2.4.G and 5.1 of the second antecedent of this resolution, to which the appropriate reference is made).

For all these reasons, the analyzed treatment calls for a special reinforcement of the

of transparency - in relation to the proportionality of the treatment - in all its

manifestations and with adequate guarantees in relation to the type of treatment, which

the instruction carried out cannot be attributed to the investigated entity, which constitutes

the violation of the provisions of article 5.1 of the RGPD.

10. Revocation of consent. Article 7.3 GDPR.

Regarding the violation of article 7.3 of the RGPD, referring to the revocation of the

consent, it must be indicated that in the agreement to initiate this procedure

it stated the following:

(...) IV.1 Establishes article 6 of the RGPD under the heading "Legality of processing", which

following: 1. The treatment will only be lawful if at least one of the following is met

conditions:

a) the interested party gave their consent for the processing of their data

personal for one or several specific purposes (...)

It establishes article 7 of the RGPD under the heading “Conditions for the

consent ", in section 3, the following:

The interested party will have the right to withdraw their consent at any time.

The withdrawal of consent will not affect the legality of the treatment based on the

consent prior to withdrawal. Before giving their consent, the interested party will be

informed of it. It will be as easy to withdraw consent as it is to give it.

In the present case, it has turned out that through the LALIGA app, a

Consent provision procedure by marking a box

that appears in a pop-up window or dialog box of the application itself. (Without

prejudice that once accepted, the device through the system functions

request individually the permission to record audio and to access

device location).

On the contrary, the procedure for the revocation of consent is

circumscribes the use of the functionalities of the operating system for the

Application permission settings. That is, there is no such procedure.

added to revoke the consent as well as the one arranged to grant it.

In short, the LALIGA app uses a procedure designed and added by the

entity, to the functionalities of the operating system, through the marking of a

box and yet lacks any procedure to revoke consent in

the same terms. The reference to the device settings that

makes LALIGA in the communications provided during the previous actions of

inspection, since it is said entity that decides to implement said procedure ad

hoc and to which it is also attributable, the absence of the same type of procedure for

revoke consent.

IV.2 In this regard, it is especially illuminating, in relation to the case analyzed, that

collected in the document Opinion GT259, of November 28, 2017 regarding

Guidelines on Consent developed by the Article 29 Working Group, –and

ratified by the European Committee for Data Protection - which indicates the following when

consent is obtained electronically with a simple click, swipe or

keystroke, data subjects should, in practice, be able to revoke that

consent just as easily. When consent is obtained

by using a service-specific user interface (for example, via

of a website, an application, an account login, the interface of a

IoT device or by email), there is no doubt that a data subject must

be able to revoke consent through the same electronic interface, since the change to

another interface for the sole reason of withdrawing consent will require effort

improper.(…) (…)The requirement of an easy revocation is described as an aspect

necessary of the valid consent in the RGPD. If the right of revocation does not meet

with the requirements of the RGPD, the consent mechanism of the data controller

treatment is considered to be in breach of the GDPR. (...) (The underlining is from the Agency

Spanish Data Protection).

IV.3 Therefore, from the actions carried out and without prejudice to what is derived from the

instruction of this sanctioning file, it follows that the way to revoke

consent raises difficulties regarding the procedure for its provision that

is limited to marking a box in the application itself, without going to the

settings in the device's operating system. (…)

The investigated entity has stated in relation to the revocation of the

consent, in short, that has created a "Subscription Center" in the application

that allows you to update the permissions granted to the application, and therefore, you can

revoke the consent for the functionalities analyzed, from within the

application and not using a device operating system procedure.

Based on the foregoing and in accordance with the principle of effectiveness, proportionality and

dissuasiveness in the imposition of sanctions, given that they have been adopted

the measures that constituted the sanction indicated in the initial agreement, the

filing of the sanction for non-compliance with art. 7.3 of the RGPD that proposed the

instructor.

11. On the principle of legal certainty.

LALIGA maintains in its arguments made to the proposed resolution, in

summary, (...) The assessment of the existence of an infringement is based on considerations

that are not taken into account by the European or Spanish legislator, given that the duty to

reporting must be carried out at the beginning of the treatment cycle, as required by

the criteria of the EDPB.

(...) being the legal framework applicable to all cases of treatment, of the

Proposal could derive that the scope and content of the information to be

facilitated to the affected party would have a variable character in attention to the circumstances that in

each case considers the Supervisor himself to be concurrent, even when there is no provision

any in the regulations that require that the way of complying with the duty of information differs

depending on whether there is a single data collection or several successive ones. Therefore, the

control authority could, before two assumptions of treatments in which it is provided

similar information, decide that in some cases the principle of

transparency, while in another the principle would call for “enhanced” compliance

of the duty of information, in terms that are not foreseen in any provision and

to be established in each case based on what the

controlling authority.

(...) Such a conclusion must be considered contrary to the principle of security

legal, guaranteed by article 9.3 of the CE. It is not possible for the Supervisor, in the

framework of some actions can modify the interpretation of the legislator, on the basis

of some considerations not foreseen by the legislator (...)

It must be based on the concept of legal certainty, which LALIGA understands violated

tenor of the pronouncements of the proposed resolution.

The Constitutional Court configures the principle of legal certainty, as a

“sum of certainty and legality, hierarchy and normative publicity, non-retroactivity of what is not

favorable, prohibition of arbitrariness, but that, without exhausting itself in the addition of these

principles, it would not have needed to be expressly formulated. legal certainty is

the sum of these principles, balanced in such a way as to promote, in the order

justice, justice and equality in freedom” (Vote 27-81). legal certainty

Understood in its broadest sense, legal certainty supposes the expectation

reasonably founded of the citizen in what should be the action of power in

application of the law” (STC 36/1991).

Likewise, the High Court indicates, the principle of legitimate expectations is a

that (...) derives from the constitutional postulates of legal certainty, regarding the act

own and good faith, and seeks to protect the company against changes

untimely that the Administration adopts, ignoring antecedents in which

that was founded to continue in the exercise of an activity or in the claim of certain

conditions or rules applicable to their relationship with the authorities (...)

Both principles provide the framework for action of individuals in their

relations with the administrative public powers, characterized by the notes of

predictability and legal certainty, contemplated in articles 9 and 103 of the

Spanish constitution.

Based on the foregoing, LALIGA's allegations regarding the bankruptcy of the aforementioned

principles must be rejected outright, insofar as it has not been issued by this

Agency, any resolution that analyzes a similar assumption, and that applies the RGPD,

it is

to say that

a certain interpretation has been advocated and now, in the present

case, it has been modified.

The allegations in this sense are expressed in the conditional, "could be derived",

“would consider”, that is, they indicate hypotheses that in LALIGA's opinion could happen.

Addresses an expectation that a disparity of criteria could occur before

similar assumptions. That is to say, it does not prove that it has occurred, but rather it states that,

your trial, it could happen. Faced with this, it must be pointed out that the legitimate and

legal certainty is “built” on the determination of the interpretation criteria

and application to the assumption of fact what is established in the norm. And as stated

before, at present there is a lack of elements in comparative terms to carry out

that statement.

As indicated by LALIGA in its arguments made to the initial agreement, the

GDPR is a new standard, in force since 05/25/2016 and fully applicable from

05/25/2018, so given its short period of application this Agency has not issued

some resolution from which a certain answer can be established a priori.

It should be noted that in any case, a general criterion is not being determined,

but the material content of this resolution is limited to this type of

treatment with the special characteristics of which it is a creditor.

Now, LALIGA, since the initial agreement, has had enough elements

to know the criterion of the supervisory body and adapt its actions to it – such

as it has done with geolocation, without explaining the difference because in that case if

includes the icon and in the case of the microphone it does not. All this without prejudice to the fact that, if

Although no similar case has been analyzed in this Agency, the truth is that the Whereas

of the RGPD offer interpretive criteria since 2016.

To which we must add that this Agency, although it has not pronounced itself in

similar resolutions, has not changed its interpretation in this regard, please cite

As an example, the document referring to “Application access to the screen in

Android devices”5, where it is indicated in its conclusions that (…) The acceptance by the

screen recording user does not meet the conditions of consent

if the interested party has not previously been clearly informed of the purposes of said

treatment in accordance with article 13 of the RGPD. Similarly, it will not comply with the

principles of transparency that the recording of the screen occurs without the user

be aware of when it is running, regardless

that consent has been granted at a given time.

Application developers, if they use screen recording, must

ensure that user consent is appropriately collected with

after complying with the information requirements indicated by the regulations and

offers an easy way to withdraw such consent. In addition, they must provide

mechanisms so that the user is fully aware of when they are

making these recordings. (…)

In conclusion, it may be that at the beginning of the LALIGA proceedings he was unaware of the

criteria of the regulatory body regarding a specific treatment, but at this point

5 https://www.aepd.es/media/notas-tecnicas/nota-tecnica-acceso-a-programa-en-android.pdf

of the procedure, it cannot be placed in a deliberate ignorance of the criterion of this

body, since it has no elements to consider that the Agency validates its action

without the inclusion of the brand or icon, quite the contrary.

12. Regarding the determination of the amount in the initial agreement and its impact on

the rights of the investigated.

LALIGA, in its arguments made to the proposed resolution, indicates, in

synthesis, that the determination in the initial agreement of an amount of the sanction, prior

assessment of circumstances of unlawfulness and culpability, without hating the entity,

places him in a defenseless position, as he cannot claim anything regarding the inaccurate

of that assessment. It also maintains that the motion for a resolution has

multiplied by 2.5 the amount established in the initial agreement, without the existence of a document or

additional proof in the instruction, assuming all this that the processing of the

procedure can be punished by the administrative body, causing a

situation in peius.

Against this, it should be noted, first, that since the entry into force of the

Law 39/2015 of October 1, the possibility of determining an amount at the beginning of the

procedure has its origin in the provisions of articles 64.f) and 85. That is, from

its validity and application (at least 3 years ago), this Agency has been acting

"procedurally" in that sense, with the corresponding prior analysis of the Cabinet

Legal of the Agency and without having been declared by any jurisdictional body

unlawful in that procedure. In addition, the principles of legal certainty and trust

legitimate, which have been invoked by the LIGA in this procedure, we

They claim that precisely a change in the configuration of the start-up agreements

would cause the bankruptcy of said principles -in the procedural field-, since it would not be justified

because in the procedures instructed by the Agency since 2016, it is carried out

one way, and when the person under investigation is LALIGA, there are circumstances that imply that

change of course. Well, in those cases, as in this one, a priori, the amount is neither

fixed - it is determined within a range -, nor the reproach of an infringing conduct

can be established only through the imposition of a financial penalty.

Second, that determination is an “initial assessment of the

circumstances” derived from the elements obtained during the previous actions of

inspection, and against what the investigated has the right to allege what his right

agrees to the appropriate procedural step, that is, in the first pleadings step.

That is why expressions such as (...) Of the performances are always indicated

practiced and without prejudice to what is derived from the investigation of this file

sanctioning (...) or (...) the sanction that could correspond for violation of the article

5.1 a) of the RGPD would be (…).

Therefore, we cannot face any type of defenselessness, precisely because

two fundamental issues, (i) it is an initial assessment, which can be

maintained, or "modified" subsequently "up" or "down" (precisely derived from

what results from the investigation) and (ii) against which the investigated maintains his

list of "procedural weapons" to refute what was indicated by the sanctioning body.

Thirdly, it should be noted that there is an additional element to assess

during the instruction, with respect to what is included in the initial agreement, such as the

recognition by LALIGA that it has not included a brand, sign or icon in the

application, and that he does not have the will to carry it out either (a situation that continues even

after the motion for a resolution).

As has been repeatedly explained, this circumstance has consequences

that increase the sanctioning reproach – and not for not giving up the procedure, but because they reveal a continuing infraction that has a greater impact on the rights of those affected. Nor can it be understood that the processing of the procedure supposes a penalty to the investigated, it serves to mention that precisely in Regarding the possible violation of art. 7.3 GDPR, the instructor proposed the file, and regarding the display of the geolocation icon, it is understood that the initially claimed. Both circumstances are the result of the instruction of the sanctioning procedure, which shows that, obviously, it cannot be understand "penalized" the investigated when processing the procedure.

13. On typical behavior.

Article 83.5 a) of the RGPD provides, that (...) Infractions of the following provisions will be sanctioned, in accordance with section 2, with fines administrative fees of EUR 20,000,000 maximum or, in the case of a company, a amount equivalent to a maximum of 4% of the total global annual turnover of the previous financial year, opting for the highest amount: a) the basic principles for processing, including the conditions for consent under the articles 5, 6, 7 and 9;(…).

The exposed facts are constitutive of an infraction, attributable to the entity investigated, typified in article 83.5.a) of the RGPD and qualified for the purposes of prescription as a very serious infringement in article 72.1.a) of the LOPDGDD, which considers as such, "the treatment of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679."

14. About the applicable corrective powers.

It establishes article 58 of the RGPD, under the heading "Powers", in its section 2 d) and i), the following:

Each supervisory authority will have all of the following corrective powers

indicated below: (…);

d) order the person in charge or in charge of the treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate, in accordance with

a certain way and within a specified period; (…)

i) impose an administrative fine under article 83, in addition to or instead of

of the measures mentioned in this section, according to the circumstances of each

particular case;

15. Of the imposition of sanctions.

It establishes article 83 of the RGPD, under the heading “General conditions for

the imposition of administrative fines “in its sections 1, 2 and 5, the following:

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

in accordance with this article for the infringements of this Regulation indicated

in sections 4, 5 and 6 are in each individual case effective, proportionate and

dissuasive

(…)

2. When deciding to impose an administrative fine and its amount in each case

individual, due account shall be taken of:

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

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

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

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to alleviate

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,

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 controller or processor reported the breach and, if so, to what extent;

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

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 mechanisms of

certification approved in accordance with article 42, and

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, through infringement.

(…)5. Violations of the following provisions will be sanctioned, in accordance with

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

of greater amount:

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

consent under articles 5, 6, 7 and 9; (…)

16. Determination of the proposed measures.

In view of the practiced instruction, of the persistent behavior of

non-compliance by the investigated entity, and attending to compliance with the

principle of effectiveness, proportionality and dissuasiveness, it is considered appropriate to propose

the imposition of the following measures for the violation of art. 5 of the GDPR, principle

of transparency:

p.

q.

The one provided for in article 58.2 d) RGPD to order the investigated entity to

that the treatment carried out through the application complies with the

transparency principle.

The one provided for in article 58.2 i) RGPD, referring to the imposition of a fine

administrative.

17. Determination of the amount of the sanction consisting of an administrative fine.

In accordance with the provisions of article 85.2 and 5 RGPD transcribed above, it is estimated

determine the amount of the penalty, according to the following criteria:

17.1 About extenuating circumstances:

In the initial agreement, derived from the previous inspection actions,

considered that the extenuating circumstance derived from section a of art. 85.2

RGPD, regarding the duration of the infringement, since only the

application on June 9, 2018.

However, derived from the instruction of this sanctioning file, and

at the procedural moment in which the proceedings are found, said circumstance

disappears, since the manifestations of the investigated entity

– that are confirmed

in the arguments made to the motion for a resolution -

indicate that they persist in their

action and that they will not include elements that reinforce the principle of transparency. For the

that we are facing a continuous infraction in the time that happens to the present,

which aggravates the sanctioning reproach in relation to the duration of the infraction.

The entity alleges that there are extenuating circumstances such as:

-The adoption of appropriate measures to mitigate possible damage and

damages by developing the app from the principle of privacy by design and by

default, self-imposed diligence and proactive responsibility. This mitigation is

corresponds to art. 83.2 c) GDPR. “Any action taken by the person responsible or

in charge of the treatment to mitigate the damages suffered by the interested parties”

-The volume of affected subjects. The 50,000 users cannot be a

large-scale number for its management of a supposed base of 10,000,000 possible

users. The figure obtained from Google Play does not allow us to infer the number of users who

have active the functionalities or the operating system that was required to be

Android 6.0 or higher. This attenuation corresponds to art. 83.2 a) GDPR.

-LALIGA has not committed any previous infraction regarding the protection of

data, this mitigating factor corresponds to art. 83.2 e) GDPR.

-LALIGA has cooperated proactively with the AEPD from the very beginning.

both through tweeter and by sending emails addressed to

instruccion@agpd.es and inspeccion@agpd.es. Also, during the inspection visit,

showed a collaborative attitude, with the presence of COMPANY 1 in order to provide

of maximum transparency to the procedure. This circumstance corresponds to the

art. 83.2 f) GDPR.

In the allegations made to the motion for a resolution, it is indicated that

adopted measures that prove compliance with the principle of privacy from the

design such as: (...) that data processing is not carried out that allows a

identification of users, not collecting any sound captured by the microphone of the

device, nor on the servers, (...) a reminder process was established

about the possibility of access to these functionalities.(...) The

possibility for the user to revoke consent, not only from the system itself

operating phone, but with an additional procedure (...) Once published the

information regarding the application, and before a warning related to the

possible investigation of the facts carried out on social networks (not aimed at

LALIGA), was made available to the control authority, The arguments of the

proposal that there is a duty to collaborate would lead to the interpretation of

that the mitigating factor provided for in art. 83.2 f) GDPR.

In the face of these manifestations, the following must be indicated:

On compliance with the principle of privacy by design:

LALIGA states that (...) no sound captured by the

microphone of the device (...) statement that must be rejected because it would count to the

truth, precisely the operation of the application is based on capturing the

sound from the microphone.

It also indicates that measures were taken to prevent the user from being identified, without

However, no coherent explanations have been offered regarding the treatment of the

IP address of the user, since, despite what is indicated in the Report, it is recognized that

controls both a priori and a posteriori said information, that is, once there is

There has been a match or concordance with the information transmitted to the servers in the cloud.

Nor has it explained the possibility of identifying a specific device and

the measures that prevent this from occurring, to the extent that when it has had

Well, he has been able to identify a device and provide a navigation record of it.

Nor has it accredited the existence and the mechanism of "reminders" about

the provision of consent for access to audio information and

geolocation, which is indicated in its current privacy policy.

Regarding the collaboration with the Agency, it was already indicated in the proposal of

resolution that (...) Finally, indicate that the reported entity has not cooperated

actively that allows applying the circumstance provided for in art. 83.2 f) GDPR. The

entity reported communicated with the AEPD after the publication by the body

on the social network twitter that ex officio investigations were being initiated. That is, it is not the

entity that communicates, motu proprio, no information, but acts behind the

knowledge of that information.

Regarding the collaboration and cooperation that he claims he showed, indicate that in

Article 58.1 RGPD collects the powers of inspection, so the appropriate one is done

Refer to sections a), e) and f). Likewise, both the old LOPD and the recent

LOPDGDD, establish in the duty of collaboration and the scope of the actions of

inspection, constituting non-compliance with a violation of the regulations. so no

it is possible to attribute to the reported entity, any conduct to which it was not

forced. It is not possible to "reward" an entity for doing what the standard determines. (…)

The argument that, according to the Agency's interpretation,

The mitigating factor of collaboration could never be applied, because as indicated by LALIGA

acts after learning that the supervisory body would initiate investigative actions.

Cooperating or collaborating requires a material content that goes beyond a mere

communication, as LALIGA did. Therefore, in this case it is fully assumed the

indications made in the motion for a resolution.

Finally, regarding the safeguards indicated in the reports of

the “external” law firms and the meetings that were held prior to

the implementation of the new functionalities, the proposed resolution indicated what

next (...) It is not appropriate to appreciate article 83.2 c) RGPD, precisely because neither in the

design took into account the safeguards recommended by external reports, nor

nor did he attend to the documentation that reflects the internal meetings in LA LIGA of

Privacy by Designa on the AppLALIGA, maintained in March 2018. (In this

documentation it is recommended to anonymize the data obtained in such a way that it is not

may be associated with any personal data or identifier. Specifically, it is recommended not

process or collect unique identifiers such as IMEI, MAC address, device id, ID of

advertising, device serial number or IP address). Arguments that are taken

entirely in this resolution.

In short, LALIGA alleges the adoption of measures that protect the rights

of users and that are privacy-by-design compliant, and have not been accredited.

Likewise, the entity has brought to the procedure to carry out a trial

comparative, the application whose purpose is to identify songs through capturing

of audio and that the device shows which composition and its author it refers to. Well

Well, as explained in the resolution, said application grants full control to the

user, since it is the user -and not the application- who decides to activate the microphone so that it

pick up ambient sound. Circumstance that would eliminate the reporting requirement

claim in this case.

On the volume of affected.

The investigated entity makes allegations to the initiation agreement, in relation to

the concept of treatment on a "large scale" that must be rejected completely, since it is

a concept that is linked to other elements referred to in the RGPD (need to

data protection delegate, and other issues... but it is not referred to the volume of

treatments as modulating criterion of the amount of penalties).

-Notwithstanding the foregoing, Ruling WP 243, indicates the following (...)

In any case, the Working Group recommends that the

following factors, in particular, when determining whether the treatment is carried out at

big scale:

a) the number of interested parties affected, either as a specific figure or as a

proportion of the corresponding population;

b) the volume of data or the variety of data elements that are the subject

of treatment;

the duration, or permanence, of the data processing activity;

c)

d) the geographical scope of the treatment activity. (…)

The aforementioned Opinion not only indicates those characteristics, which would be perfectly

applicable to the alleged object of analysis in this proceeding, but also

proposes as examples of "large-scale" treatments, some treatments where the

geolocation is decisive, as is the case in the system designed by LA LIGA to

fulfill the intended purpose.

Similarly, as in the previous case, the persistence of their offending behavior

it obviously keeps (even increases) the number of those affected,

as discussed in the section on aggravating circumstances.

About the absence of violations.

The absence of infractions cannot be taken into account for the purposes of

of the entity to accommodate section e), as this expressly indicates

(…) any previous infringement committed by the person in charge or the person in charge of the treatment

(…)

That is to say, the term absence does not appear in the norm, from which it is deduced that the

previous infractions committed, would determine the concurrence of a circumstance

aggravating circumstance to assess, but the absence of infractions, in the present case cannot

have mitigating effects, since the normal thing is not to commit infractions.

On the redefinition of the privacy policy.

It is accredited that the obligations derived from article

13 RGPD and 11 LOPDGDD, even explaining the logic of the treatment. Nevertheless,

the foregoing, cannot have the intended effects, in the first place, since giving compliance with a standard cannot be assessed in a procedure sanctioning, - above all, when the violation of said precepts - and regarding the explanation of the logic of the treatment, it does not fill the gap regarding the absence of the brand, icon or sign.

About geolocation icon sign.

It is credited that an icon is displayed when geolocation is activated, circumstance that mitigates the unlawfulness of the imputed infringement and that, obviously, will have effects in determining the amount to be imposed.

17.2 Regarding aggravating circumstances:

17.2.1. Section a) establishes the nature, seriousness and duration of the infringement, taking into account the nature, scope or purpose of the data processing operation concerned, as well as the number of affected parties and the level of damage and damages they have suffered;

Regarding the nature of the infraction, it should be noted that we are facing the Violation of an essential informative principle in the treatment of personal data personal, as it is configured as the cornerstone on which rest other principles and that transcends all areas of the right to data protection. Of Hence, non-compliance is of special importance.

In relation to the seriousness of the infringement, it must also be observed, as parameter, the number of affected, the entity stated during the previous actions of inspection, which are 50,000 users who have accepted the treatment in question, and derived from the persistence over time of the offending conduct, cannot be considered that this number has decreased, but that, within that limit, there may have been other users who have been recorded and geolocated.

This argument is confirmed in view of the explanation offered by LALIGA in the

documentation that accompanies the motion for a resolution, when referring to the manner of

select the users, which supports the renewal of “the sample”, which follows the order

connection to the server. It is indicated that the sample is established “at a specific moment

and remains in effect indefinitely. (...) at the request of LALIGA, they could be modified

the indicators mentioned above, so that new users are included in the

sample".

Also in relation to the number of affected, LALIGA indicates in the

allegations to the proposed resolution that, within the group of 50,000 users,

they are applying the functionalities to 4,227,848. circumstance that can not have

intended effects, because taking into account the possibility not only of using the

information of the 50,000 users, but to put it into operation for any

user who has granted the permissions to LALIGA through the operating system, said

circumstance does not eliminate the sanctioning reproach.

Based on the foregoing, and after rejecting the arguments referring to the concept of

“large-scale” treatment proposed by the investigated entity in relation to the

volume of data, and the irregular nature of the sample at the will of LALIGA, it is estimated

that the indicated figure constitutes by itself - free of other probabilities pointed out -

an aggravating circumstance.

17.2.3. Sections b) and d) establish (...) the intent or negligence in the

infringement; (...) the degree of responsibility of the person in charge or of the person in charge of the

treatment, taking into account the technical or organizational measures that have been applied

under articles 25 and 32; both sections are related to the element

subjective in the commission of the offence.

The opening agreement indicated the following (...) both sections were

relate to the subjective element in the commission of the offense. remember

that culpability consists in the capacity of the obligated subject to act in another way,

that is, in accordance with the legal system. The analysis of the principle of culpability

and due diligence in data processing is carried out through the premise that

the establishment and start-up of the functionalities under analysis,

respond solely and exclusively to LA LIGA and therefore the breaches indicated in

throughout this initiation agreement, are attributable to it at least by way of

culpable negligence. (...).

The motion for a resolution indicated the following (…) In the phase

procedural in which the procedure is found and as a result of the allegations

formulated by the investigated entity, which show the persistence in the

offending conduct, undoubtedly already with full knowledge of the criteria of the agency

regulator, from the reports of the Working Group of Art. 29, cannot be maintained in the

same conditions the assessment of this circumstance, but inevitably it has been

to raise the sanctioning reproach, based on what was already indicated in the aforementioned agreement of

opening and the current situation, where the entity persists in committing the infraction,

Specifically, in the aforementioned opening agreement it was indicated (...) there is a serious lack of

diligence in data processing to the extent that the entity was fully

aware of the implications that the right to data protection had the

application, so much so, that expressly in one of the reports requested by the

entity indicated precisely the need to establish mechanisms that

allow the user to identify that the treatment in question was taking place. Y

Despite these considerations, nothing was included in that sense. The mere request of

legal reports in order to analyze the implications for privacy arising from the

use of the application, without taking into consideration the safeguards that are established,

they reduce this advice to a mere formality, they prove a deliberate non-observance

of these implications and cannot be taken into account as parameters that mitigate

guilt or unlawfulness of the imputed conduct, but rather aggravate the disregard of

the infringing action and in identical terms the sanctioning reproach. this circumstance

becomes a qualified aggravating circumstance. (...).

Likewise, in terms of compliance with the principle of privacy by design

and by default, as noted above to counter extenuating circumstances

proposed by the entity, there is in the procedure, documentation that reflects the

internal meetings in LA LIGA of Privacy by Designa on the AppLALIGA, held

in March 2018. (In this documentation it is recommended to anonymize the data

obtained in such a way that it cannot be associated with any personal data or identifier. In

In particular, it is recommended not to process or collect unique identifiers such as the IMEI,

MAC address, device id, advertising ID, device serial number or IP address).

In relation to these principles and taking into account this safeguard, the

entity states that the IP address and the user agent are no longer used, and

however, it was verified during the instruction of the procedure that, in the policy

of privacy hosted on the web, appears in identical terms that, in the month of June

2018, when the exploitation of the application began, (folios 27 and 351). That is, if

reports that the IP address is collected and a user identifier is assigned.

Ultimately, based on the subjective element in the commission of the offence,

one cannot speak of a serious lack of diligence, but rather that the entity, despite the

exposed conditioning factors, voluntarily persists in its action with the explanation

of the "consideration judgment" that has been carried out in this regard, to which the appropriate

referral and that must be rejected outright in accordance with the arguments that

they were exposed on the basis of law that refutes it.

All of the above implies a very serious lack of diligence in their actions and

no evidence to presume implementation of any type of measure or improvement that

make sure that the valued events do not happen again.

The required diligence is given to us by the offender's professionalism, that is, the

activity to which it is dedicated, and that, although the LIGA does not have as its main activity the

treatment of personal data, the truth is that with the application there are

important implications in the matter, so it should be greater when,

precisely, it has the implications referred to throughout this resolution.

This has been collected in the Judgment of the National Court of Appeal 104/2006

points out that "the applicant entity for the activity it carries out must deal with a large

volume of personal data in its files, which means that extreme care must be taken

in the handling of said data to achieve effective protection, since a

autonomous fundamental right, the right to the protection of personal data according to the

STS 292/2000".

In the same sense, the Judgment of the National High Court, Appeal 143/2006

points out that "that's right, the decrease in the guilt of the sanctioned person or the

illegality of the fact, since the nature of the activity carried out by the entity

recurrent, and its permanent relationship with personal data, determines that the

behavior required of those who are usually in contact with this type of data

be distinguished and exquisite care about compliance with the requirements imposed

by the LOPD, because the protection of fundamental rights is at stake - art. 18.4

EC-. “

17.2.4. Section k) establishes any other aggravating or mitigating factor applicable to

the circumstances of the case, although the imputed entity does not have as its main object of

business the processing of personal data, the truth is that to exercise your

interest in protecting their financial assets from fraud (rights to exploit the

issuance of the football matches of its associates) uses the treatment of the data of

users through invasive techniques of their privacy for the fulfillment of that

purpose, without the certainty of the effectiveness of its system, for example, in terms of the location and

to the impossibility of determining if the user is in a bar on the street or in

a private home or dwelling located at any height in the same vertical of the

establishment.

This system may not fulfill its purpose as the device may be in

another altitude that the system is not able to discriminate. It may happen that the device

is in a multi-storey building, capturing information at the private address of

a third party, and that associates the information processed with that of a place in which it is not

find. The investigated entity does not explain in what terms its system is modified with

the new “heat map” that it claims to have introduced.

In the allegations made to the proposed resolution, LALIGA credits

a modification of the privacy policy that is accessed from the website itself

app. However, due to its own operating system, which is

activates the functionalities object of analysis, during the broadcast of football matches of

LALIGA teams, said privacy policy cannot identify the specific moment

of sound pickup. Hence, no matter how well defined the policy of

privacy, the brand, signal or icon will always be necessary, showing the user that

the audio captured by the device's microphone is actually being accessed. (except

that it be the user himself who decides its activation, as happens in other applications

of similar operation).

17.2.5. Persistence in the actions of the investigated entity that continues to fail to comply

the art. 5.1 a) of the RGPD, obviously influences the determination of the amount of the amount

of the fine to be imposed.

Because it affects the (i) period during which the infringement occurs, which eliminates the

only extenuating circumstance observed in the initial agreement, to make it a circumstance

highly qualified aggravating circumstance: the commission of the infraction is passed in at least one day,

to the commission of the offense for several months, and that exponentially increases the

sanctioning reproach and therefore the amount of the amount to be imposed, since at least

from the start of the national league championship, until the month of January 2019 – which is

the date on which LALIGA states that it continues without including notice, mark or sign on the

capturing the audio- there have been

days of the aforementioned championship (without prejudice to other competitions that may

organize LALIGA), with an average of 3 days of broadcasting matches for each of

those days, there have been at least 57 days of broadcasting soccer matches;

– until the motion for a resolution – at least

(ii) this circumstance of the period during which the infringement occurs also

has been able to increase the volume of those affected (the limit of 50,000 users in a

day of use of the functionalities cannot affect the same users who

for at least 57 days of issuance. The maximum number may be the same, but

they do not have to be “the same” users – given the device choice system

- and therefore the consequences of the lack of transparency would affect more people);

and finally indicate that obviously, the persistence in the commission of the

infraction influences the assessment made of the (iii) subjective element in the commission

of the infraction that eliminates the culpable negligence initially considered for

also turn it into a very qualified aggravating circumstance.

17.2.6. These circumstances – which were included in the motion for a resolution and

maintained in this resolution - prevented maintaining the amount of the sanction to

impose on the terms of the startup agreement.

Now, it has been proven regarding the use of geolocation, that

an icon is actually displayed, so the amount that was included in the proposal

of resolution (500,000 euros) must be reduced, without prejudice to the persistence in the

commission of the offense regarding access to the information captured by the microphone without

any mark or sign.

17.2.7. Therefore, it is estimated that the amount of the penalty to be imposed is 250,000 euros,

all in relation to the provisions of article 85.1 RGPD in that the

imposition of the sanction must be effective, dissuasive and proportionate.

As for effective and dissuasive, it must be taken into account that the imposition of the sanction

supposes the “punitive” response of the public power in the face of illicit conduct, and has, among

others, the purpose of influencing the will of the sanctioned person to prevent him from repeating

commit the offending type and for legality to be restored.

In view of the persistence in committing the offense by the

LALIGA, taking into account the amount of the penalty indicated in the proposal

of resolution, it is estimated that the sanction proposed in this procedural phase is

adequate to the intended effect and complies with the dissuasiveness.

The determination of this amount is estimated adjusted to the judgment of

proportionality, for which three elements have been taken into account: the concurrence of

aggravating or mitigating circumstances; the economic effect on the assets of the

sanctioned and the percentage that the proposed sanction supposes, in the range of amounts

that determines the norm.

b)

taking into account the concurrence of aggravating circumstances

qualified, and the absence of extenuating circumstances – except for what refers to the

geolocation icon sign -; the exponential increase of reproach

sanctioning when passing from the commission of the infraction of one day, to at least 57 days of

broadcast of matches.

c) Continuing with the judgment of proportionality, it must be taken into account

the amount of the sanction, with the effect pursued with it and the possible loss

or economic affection in the patrimonial sphere of the sanctioned person.

In this case, it appears on folios 274 to 348, the Audit Report, Annual Accounts

and Management Report of LA LIGA, as of June 30, 2018, including a

Net amount of turnover of 1,754,301,000 euros. So the

imposition of a penalty in the amount of 250,000 euros, in no way can

consider disproportionate.

d)

And finally, the percentage that it represents within the range of the amount

determined by the RGPD for this type of infraction (which the LOPDGDD considers

"very serious") and amounting to 20,000,000 euros. The proposed penalty

about 1% of that amount.

17.2.8. Persistence in the actions of the investigated entity that continues to fail to comply

the art. 5.1 a) of the RGPD, and in view of the principle of effectiveness and dissuasiveness, makes

a sanction is imposed in accordance with the provisions of article 58.2 d) ordering that

the treatment carried out is adapted to the RGPD through mechanisms that reinforce the

knowledge by users of the activation of the functionalities of

microphone and location of the devices that install the application, at the time

that this occurs, with the warning of the provisions of article 85.6 of the RGPD

which determines that (...) Failure to comply with the resolutions of the control authority to

pursuant to article 58, section 2, shall be sanctioned in accordance with section 2 of the

this article 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

of greater amount (...)

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 NATIONAL PROFESSIONAL FOOTBALL LEAGUE, with NIF

G78069762, in accordance with the provisions of article 58.2 j) of the RGPD, a penalty for

the commission of an infringement of article 5.1 a) of the RGPD, provided for in article 83.5 a)
of the aforementioned RGPD, consisting of an administrative fine, in the amount of 250,000 euros
(two hundred fifty thousand euros) in accordance with the provisions of article 83. 1, 2 and 5
of the GDPR.

SECOND: ORDER to NATIONAL PROFESSIONAL FOOTBALL LEAGUE, with NIF
G78069762, in accordance with the provisions of article 58.2 d) of the RGPD for the infringement
of article 5.1 a) of the RGPD, provided for in article 83.5 a) of the aforementioned RGPD, which: adapts
to the principle of transparency the use of the application in the terms indicated in the
this resolution, through mechanisms that reinforce the knowledge on the part of
users of the activation of the microphone functionality of the devices that
install the application, at the time it occurs. All this must
effective within ONE MONTH.

THIRD: FILE the NATIONAL PROFESSIONAL FOOTBALL LEAGUE, with NIF
G78069762 the imputation of the commission of the infringement of article 7.3 RGPD, foreseen
in article 83.5 a) of the aforementioned RGPD

FOURTH: NOTIFY this resolution to the NATIONAL FOOTBALL LEAGUE
PROFESSIONAL.

FIFTH: Warn the sanctioned person that he must make the imposed sanction effective once
that this resolution is enforceable, in accordance with the provisions of art.
98.1.b) of Law 39/2015, of October 1, of the Common Administrative Procedure of
Public Administrations (hereinafter LPACAP), within the voluntary payment period

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

Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003, of 17

December, 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 Data Protection at Banco CAIXABANK, S.A. Otherwise, it

will proceed to its collection in executive period.

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

on the 1st and 15th of each month, both inclusive, the deadline to make the voluntary payment

will be until the 20th day of the following month or immediately after, and if it is between

On the 16th and last day of each month, both inclusive, the payment term will be until the 5th of

second following business month or immediately following.

In accordance with the provisions of article 50 of the LOPDPGDD, 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

LOPDPGDD, 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 period of one month from the

day following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court, with

in accordance with the provisions of article 25 and section 5 of the additional provision

fourth of Law 29/1998, of July 13, regulating the Contentious Jurisdiction-

administrative, within a period of two months from the day following the notification

of this act, as provided for 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 interested party

states its intention to file a contentious-administrative appeal. If this is the

In this case, the interested party must formally communicate this fact in writing addressed to

the Spanish Agency for Data Protection, presenting it through the Registry

Electronic Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through

any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of 1

October. You must also transfer to the Agency the documentation that accredits the

effective filing of the contentious-administrative appeal. If the Agency did not have

knowledge of the filing of the contentious-administrative appeal within the period of

two months from the day following the notification of this resolution, I would

The precautionary suspension has ended.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan 6

28001 - Madrid

http://www.aepd.es

https://sedeaepd.gob.es