 Procedure No.: PS/00416/2019

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and in

based on the following

BACKGROUND

FIRST: On 09/03/2018, this Agency received a claim

presented by A.A.A. (hereinafter the claimant 1), against the entity MIRACLIA

TELECOMMUNICACIONES, S.L., with NIF B85623775 (hereinafter MIRACLIA or the

claimed), for the use of your personal data to make a joke using

for this from the application "***APPLICATION.1", by phone call to your mobile line

***PHONE.1 in which a person pretended to be a police officer, which took place on

day ***DATE.1. For this reason, he denounces the recording made without his knowledge or

consent, dissemination of said recording to third parties, also without your consent, and

that the call is from a hidden number. Add that the line enabled as

contact by that company is an additional fee, which entails a cost for the

interested party who intends to contact it. You confirm that you have a copy of the

recording, which was provided by the person who used the services of MIRACLIA and requests

that your data be canceled, as well as the opening of a sanctioning procedure.

This claim was transferred to the MIRACLIA entity. In response to what

manifested by claimant 1, MIRACLIA informs this Agency that the joke to which

the claimant refers to is foreign to the application “***APPLICATION.1”, in whose catalog of

jokes there are none that have to do with police.

On the treatment of personal data, it indicates that it does not store data of the

overwhelmed (hereinafter also interested or person receiving the prank call):

no recordings and no phone, which will be on the prankster's mobile device (hereinafter referred to as

also, application user or person ordering the prank call); limiting himself

to provide a service to the user of the application (the joker) who chooses the joke, enters the

recipient's telephone number and, prior acceptance of the terms and conditions, generates the

recording. MIRACLIA, therefore, has no way of knowing if the claimant has received a

“***APPLICATION.1” prank (warns that there are other similar applications),

and can only block the telephone line number of the overwhelmed, still not knowing if

has actually received the joke, or delete the URL of the recording if they have it,

something that does not happen in this case as it was not provided by claimant 1.

According to MIRACLIA, it is the prankster who can erase the recording, so the

The claimant's request must be addressed to the claimant. The action of the entity, which does not identify

annoyed people, consists in preventing the recipient of the joke from receiving

more calls in the future, blocking the phone, or deleting the recording

using the URL of the prank, which has no associated phone, and as long as the

prankster hasn't done it previously.



The app user or prankster is warned twice about the

responsibility involved in making the recording.

Finally, MIRACLIA informs that since the full application of the Regulation (EU)

2016/679, of the European Parliament and of the Council, of 04/27/2016, regarding the Protection of

Natural Persons with regard to the Processing of Personal Data and the Free

Circulation of these Data (hereinafter RGPD), has modified its operations in order to

of not keeping any type of data, leaving these in the users' phones,

being impossible to identify the overwhelmed. In the event that the latter

overwhelmed, they provided their line number, they could be blocked so that they do not

receive calls in the future.

SECOND: On 07/04/2019, this Agency received a claim

presented by B.B.B. (hereinafter the claimant 2), against the entity MIRACLIA,

noting, like claimant 1, that he has been the subject of a joke (thanks

for his vote for XXXXX) that was recorded and broadcast on social networks with the mention of his

name, carried out using the application "***APPLICATION.1" (provides the link to the

audio object of the complaint –"***ENLACE.1", which allows access to the audio

corresponding to the call). Request removal of your telephone line number

mobile in which he received the call from the database of the responsible company and the

removal of audio from the network. It also denounces that xenophobic messages are made

of the supposed "association of friends of XXXXX".

THIRD: The claims to which the proceedings refer were admitted to

Processing through resolutions dated 11/20/2018 (relating to claimant 1) and 08/09/2019

(the one related to claimant 2).

FOURTH: In view of the facts denounced in the claim and the documents

provided by claimant 1, the General Subdirectorate for Data Inspection proceeded to

carrying out preliminary investigative actions to clarify the facts

in question, by virtue of the investigative powers granted to the supervisory authorities

in article 57.1 of the RGPD Regulation, and in accordance with the provisions of the Title

VII, Chapter I, Second Section, of Organic Law 3/2018, of December 5, of

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), to which the claim made by claimant 2 was also linked.

As a result of these actions, the report prepared by the inspection

acting reveals the following:

1. Information request made to MIRACLIA on various aspects, with

Dated 06/25/2019, a letter from said company was received at this Agency

in which he makes the following statements:

a. At the end of the prank call, the recipient hears a voiceover offering

the possibility of not allowing the generation of the file with the recording of the

joke. The speech is as follows:

"A friend of yours has played a prank on you. In case you don't want your

friend can listen, download or spread the prank, or in case they don't

want to receive more pranks, press 5 with your keyboard after the signal.

beep”



They add that additionally, the joke can be eliminated knowing the url of

the recording of the prank and sending an email to ***EMAIL.1 indicating that

url.

b. Among other technical aspects, they indicate that, once the prank has been programmed, the

call is initiated from the Voice over IP servers of the one claimed in the

specified date and time.

The joker user downloads the application and accepts the terms and

conditions of it. At that moment your user profile is generated

to use a Voice over IP service and a number is assigned, the

which is rented to you while you are a user of the application and make each call.

To make use of the application, choose a prank from the catalog and enter the

prank recipient's phone and schedule a date and time, and the

Voice over IP call leaves the servers in the cloud at that time you have

programmed user prankster.

If the prankster selects to record the call (and the recipient of the call,

when receiving the call does not choose the option not to record as indicated in

the previous point), an audio file will be generated with the content of the

same. The generated audio file is available at a URL to which

only the app user prankster has access and only the

prankster on your own device where you have installed the app has

associated that content to the telephone number of the recipient of the call, since

the servers of ***APPLICATION.1 do not store any personal data of the

recipient of the call.

c. In the terms and conditions of use of the application, users are informed

prankster users that the company could delete their profiles (including

contents/recordings) after 6 months of non-use of the application.

2. In order to determine the exact operation of the application and the possible

variations incorporated in the application since the last claim, the inspector

installed the application “***APPLICATION.1” on his mobile terminal. The app consists of

3 tabs: “List” (of jokes available), “Examples” and “My jokes”. In this

last tab is where pranks made by prankster will be saved if not

they are eliminated.

It is verified that in the list of available jokes there are jokes

related to claimant 1 and claimant 2.

3. On September 6, 9 and 12, 2019, the Inspection Services of the

Agency carried out tests consisting of downloading the application

“***APPLICATION.1” in a mobile terminal and proceed to its use. As a result of

these tests were obtained the findings that are outlined in the Fact

Tried Second.

4. It has been verified that the web page “***APLICACIÓN.1.es” offers a system

free and immediate to include a phone number in the phone list

blocked. According to MIRACLIA statement, the telephone number is stored

encrypted on their systems.

A test was carried out registering the telephone number corresponding to the

second SIM of the inspector's terminal, and then an attempt was made to perform a

prank this phone number. The application did not allow the execution of the prank.



5. Regarding the issue of spreading the joke, which is present in the

complaints, it should be clarified that MIRACLIA does not have any public site

where they are published or any platform for the dissemination of jokes. the jokes only

they can be spread by the prankster user by sending the link to the prank file.

audio: in the list of jokes made by the joker, next to each of the

pranks not removed by prank receiver following procedure

indicated, an icon appears to download the audio file of the recording of the

telephone conversation of the prank, another to listen to it and a third to

share it (the link to the audio file of the recording is sent through the

that has been chosen to share it - this is the only moment in which the

prankster knows the link to the audio file).

6. On 08/26/2019, the Inspection Services accessed the website

“***WEB.1”, to the URL corresponding to the recording of the joke made to the

claimant 2. It is verified that using the right button shows different

options, including playing and downloading the recording.

The current inspection includes in its report a review of the evidence of

operation of the application "***APPLICATION.1" made on the occasion of some

previous action carried out by the Agency (file E/02003/2018). With respect to

treatment by the claimed party of the personal data of the recipient, in said

report indicates the following:

YO.

YO.

YO.

Recipient's phone storage. The phone number is stored

recipient in the systems of the claimed until the moment of carrying out the

call. Prank calls can be instant or scheduled

specifying date and time of execution.

Joke recording. It remains in the systems of the claimed until the

prankster decides to delete it, the recipient of the prank decides to exercise his right of

deletion, for which you must know the web link to the prank, or as a rule

In general, a period of time of 6 months of non-use of the application established by

the claimed one.

There are no other personal data of the recipient in the systems of the claimed

of the joke additional to those reflected in the previous points I and II.

FIFTH: On 11/19/2019, the Director of the Spanish Agency for the Protection of

Data agreed to initiate a sanctioning procedure against the MIRACLIA entity, in accordance with

the provisions of article 58.2 of the RGPD, for the alleged infringement of articles 13 and 14

of the RGPD, typified in article 83.5.b) of the aforementioned Regulation; and for the alleged infringement

of article 6 of the RGPD, typified in article 83.5.a) of the aforementioned Regulation;

determining that the sanction that could correspond would amount to a total of 100,000.00

euros (50,000.00 euros for each of the alleged infractions), without prejudice to what

result of the instruction.

Likewise, for the purposes provided in article 58.2.d) of the RGPD, in said agreement

At the beginning, it was warned that the imputed infractions, if confirmed, may lead to the

imposition on the MIRACLIA entity of the obligation to adopt the necessary measures to

adapt the processing operations to the personal data protection regulations

that it carries out, the information offered to its clients and the procedure through which the

they give their consent for the collection and processing of their personal data;



all with the scope expressed in the Legal Foundations of the repeated agreement of

beginning of the procedure and without prejudice to what results from the investigation.

SIXTH: Once notified of the aforementioned initial agreement, MIRACLIA presented a brief of allegations in

who requests the reduction of the sanction referred to in the agreement of

opening of the procedure, taking into account the allegations made and the measures

immediate adopted. He bases his claim on the following considerations:

1. As a preliminary matter, the aforementioned entity warns that it has been the object of several

prior sanctioning procedures (for lack of consent

only), which are being reviewed before the Supreme Court, three of them already

formally admitted for processing and pending oral hearing. In these procedures,

discusses MIRACLIA's position in the personal relationship between prankster and overwhelmed by

facilitate a means of leisure between individuals, as well as the existence or not of personal data and the legal basis of the treatment (the legitimate interest, according to the entity), because otherwise the fact of playing a joke would not be possible. Accompany a copy of one of the resources of cassation, in which, according to MIRACLIA, their arguments are summarized.

As a result of these cases, and the entry into force of the RGPD, it made a modification of its systems to prevent data from being stored on MIRACLIA servers, moving away from the idea of "treatment of personal data" and betting, according to their demonstrations, for being a means of communication such as a telephone line. It is an intermediary in a relationship between individuals, being the user who spends the joke the responsible for the information. He is also the one who introduces the phone.

MIRACLIA indicates that it only provides security to the process, but is not capable of identifying the overwhelmed or link you to any other data; does not save the phone to which the joke does not associate it with the audio file, which is encrypted with a code. Add that blocks the phone of the recipient of the prank when he requests not to receive them, deletes the recording when requested and does not have phone lists of overwhelmed, recording lists or similar.

It is something similar, says MIRACLIA, to what happens with Instagram or Twitter when an individual takes a photo and uploads it to these social networks, which are not responsible for these facts and, at best, enable means to request the removal of the content. Either a company dedicated to sending surprise gifts has to ask for permission prior to addressee. Otherwise, the activity would not be possible.

2. In relation to the claim made by claimant 1, he reiterates that the joke on the that it refers to is not in the catalog of pranks of ***APPLICATION.1.

Regarding the second claim, it states that the interested party did not address the entity to request the deletion of your data and that this request could be made from the moment of the call or later, by having the URL with the recording. According to

MIRACLIA, this complaint shows that what is usually requested is the suppression of the joke. In this case, almost three months passed, when on the same day one could have satisfied the right.

3. About the tests carried out by the inspector:



- The recording is not materialized in an audio file with its corresponding URL until the calling user confirms that they have accepted the Terms and Conditions a second time and generates the audio file.

- The deletion of jokes occurs with the sending of a DTMF tone during the called, that the operators must guarantee its operation. Unfortunately in the VoIP world (which is the technology with which operators provide the service of sending phone calls from the servers of ***APPLICATION.1), this does not it is always like this depending on the path that the call has followed, which is behind of the instability that the system may have.

- The usability of deleting after holding down is something that MIRACLIA considers intuitive because many messaging apps do it the same way. It's about already of a usability standard for smartphones.

- The phone number for programmed pranks is stuck with the call to realize. When this is done, it disappears from the systems. In any moment the phone number and the recording are saved at the same time and place, with which is impossible for there to be an association between both data. The recording file spawns when the prankster accepts its spawn, which only occurs when the

call has ended and the prankster has not pressed the 5 key. If the prankster does not accept the generation of the recording, there is no conversion of the audio into a file accessible via URL and, therefore, not even the user could access the file. The audio would be a few bits in temporary memory without generating a closed audio file.

4. On the operation of the application: the information and the legal basis that legitimizes the data treatment.

Questions that the information can be considered personal data, since MIRACLIA is unable to identify the overwhelmed in a simple way and without disproportionate means, from the mobile phone number or voice files (STS 2484/2019: “a natural person is not considered identifiable if such identification requires time or disproportionate activities”). In this case, the only one who can identify the overwhelmed is the user and for MIRACLIA the recipient is anonymous.

Regarding the duty of information, it states the following:

MIRACLIA adopted additional measures to guarantee the security of the information processed and that the phone number was stored on the user's device and not on the entity servers. Initially, the phone of the overwhelmed was stored to facilitate any request for information from the affected party, although, according to MIRACLIA, in a irreversible encrypted with sha-2 algorithm avoiding the use of the number for any action that it was not to give that support, since it could only be recovered if someone (eg: the own overwhelmed) made it easy.

At the same time, an informative note about the treatment of data that, although it is true that the current announcement does not report everything required in the article 14 of the RGPD, it does indicate how to oppose the processing of data and its deletion (he insists that he considers that he does not process personal data, but, "ad cautelam", he informs and offers guarantees).

Likewise, in the privacy policy inserted on the website and in the Terms and Conditions

The app reports the following:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/61

“Miraclia does not collect data from the recipients of the pranks. Miraclia's activity is the

to provide a means of telecommunications so that the owner of the telephone that is downloaded

the app, choose a prank and record it, leaving the data related to the recipient of the call

stored in the user's own terminal without Miraclia keeping information about the

recipient's phone number. Miraclia provides a storage service in the

cloud of the client's audio files and at no time does it broadcast or share with

no one that information, since it is private information of the user of the application”.

On the other hand, on the occasion of these proceedings, knowing the imputation made

for the first time in relation to the information defects, has immediately proceeded to its

remedy by completing the information offered at the end of the prank conversation

as follows:

- That someone has played a joke to have a good time for both of them.

- That for the same has used the application ***APPLICATION.1 property of

MIRACLIA TELECOMMUNICATIONS, S.L.

- That to oppose said prank reaching the prankster and to suppress it can

press key 5.

- Who has more information by pressing the 1 key.

And pressing key 1 offers a detailed explanation, also included on the web. of this

In this way, from the information that it did not provide to the interested party, it has now included:

- The identity of MIRACLIA

- The contact details of the Data Protection Officer

- The term of conservation

- The basis of legitimation

- The exercise of the rights in full, although those of opposition and

delete (and also access when requested) are now specified

formally.

This is layered information included at the end of the conversation, in the Terms and

Conditions of the app, on the entity's website and in the frequently asked questions section. Contribute

the detail corresponding to the information inserted in the “Frequently asked questions” section

from the website:

“12.- I don't want to receive any more jokes. What should I do?

If you don't want anyone you know to send you jokes again, all you have to do is enter

Block my number and include the phone number. The phone number that

enter will be blocked on the platforms so that no one can ever

send a prank from this application (or of course, any other type of action). The

No. is stored encrypted in the systems, so that no one can retrieve that

# for future use.

“16.- How can I delete a joke?

Jokes are deleted by holding down your finger for a few seconds on the joke in

question".

It clarifies, next, that the foregoing does not imply its agreement with the infraction or with the

sanction, but since this is not an aspect that has been neglected in bad faith or with

purpose of avoiding any compliance, it is included again "ad cautelam" in an

immediately for correction.

C/ Jorge Juan, 6

28001 – Madrid

On the legal basis of data processing, it states the following:

Consent cannot be the legal basis for playing a joke because it is

would undermine the very fact of playing a joke or the surprise effect, as well as

It occurs in countless cases, such as sending flowers or uploading photos of friends to social networks.

social. In the latter case, the rights of deletion and opposition are guaranteed, but the

responsible for the social network does not request the consent of the people whose data is

uploaded to it by other users.

For this reason, MIRACLIA defends the origin of legitimate interest as a basis for legitimation.

ex article 6.1.f) of the RGPD. For this purpose, the corresponding test of

weighing required, following the recommendations of the extinct Working Group of the

article 29.

Moreover, it has been assessed that the legal basis is the execution of the contract between the user and

MIRACLIA, but the overwhelmed man is not a party to said contract.

It is accompanied, for these purposes, by a report that justifies the origin of the legitimate interest as

basis that legitimizes the processing of data and in which it concludes that, beyond cases

punctual in which the overwhelmed person feels annoyed (which are testimonial cases), there is no

risk to people because all security measures have been taken to

guarantee the security of the process, because the deletion of the joke is guaranteed if the

overwhelmed requesting it, the blocking of your phone and because now it has also included the

complete information.

It adds that the recording of a conversation between individuals, when the person recording is one

of the participants in the conversation, is not illegal, according to the Constitutional Court

in its judgment of November 29, 1984, STC 11/1984, when it establishes, among other things

considerations that "Whoever records a conversation of others is attentive, independently

of any other consideration, to the right recognized in art. 18.3 CE; on the contrary, who

records a conversation with another does not incur, by this fact alone, in conduct contrary to the

cited constitutional precept.

In the case of ***APPLICATION.1, the calling party is aware of the

recording of it. The user could record the conversation with a tape recorder, with the

own mobile or using applications that record conversations. Instead use

a medium (***APPLICATION.1, which provides the service). That call occurs in a

domestic environment between individuals to whom the data protection legislation does not

it affects.

If MIRACLIA, just as it had been doing until recently and is now taking up that

practice reports the recording, is providing greater guarantees (the overwhelmed

you can choose to delete the recording, delete it later, lock your phone and prevent

dissemination of the joke by the user)

5. On the measures adopted and the graduation of the sanction

MIRACLIA highlights that the claims filed with the Agency represent a

tiny percentage (0.00002%), compared to the hundreds of users it has served through



of different ways (web, final locution after the call and customer service); that

has corrected the lack of information by completing the terms provided in article 14

of the RGPD, although it considers it essential that it did offer the possibility of opposition and the

deletion of data; and that the proposed sanction would force the closure of the company, for

how much represents 25% of its turnover, which amounted to 476,000 euros in 2018,

in which losses occurred.

Requests a downward revision of the proposed sanction and, for such purposes, considers that it must

take into account the following:

. That we are in a leisure environment that does not harm the overwhelmed, nor is

misuses your personal data.

. The only data in dispute is the telephone number, which MIRACLIA does not keep, and a recording

that only the user can generate and distribute, which the entity cannot join to the non

Exist any file with phone and recording.

. That the intention has always been to comply with the norm, guarantee the security of the data and

Minimize information as much as possible.

. That it has never failed to respond to requests for deletion.

. Until the present proceeding, the infringement has focused exclusively on the

absence of consent, without imputation for non-compliance with article 14, which seems

excessive considering that it has been reporting and has proceeded to correct it.

. It has been willing to cooperate with the Agency at all times and has facilitated the

information that has been requested.

. In the process that is analyzed, the overwhelmed is always chosen by the user of the

application, who is responsible for making good use of it.

. That the question on the legal basis of the treatment is being discussed in the Court

Supreme, who will decide if the treatment is anonymous for the entity, if the

security guarantees and if it is a medium that individuals use in their lives

private.

MIRACLIA provides a copy of one of the appeals filed before the

Supreme Court in 2019, based on the following reasons:

1. Play a joke through an application or a medium in which the user is

sovereign of the information that is provided is an act developed in the domestic or

personal and therefore is excluded from the scope of protection of the regulations of

Data Protection.

2. The voice is not personal data if it does not allow its owner to be identified or if it is necessary

make disproportionate efforts to identify you.

3. The legal basis of data processing (if it is estimated that we are dealing with data

personal) by an application that provides a means of entertainment in the personal sphere

or domestic of persons is based is the legitimate interest.

SEVENTH: On the other hand, through the "Internal Market Information System" (in

hereafter IMI), regulated by Regulation (EU) No. 1024/2012, of the European Parliament and of the

Council, of October 25, 2012 (IMI Regulation), whose objective is to favor the

cross-border administrative cooperation, mutual assistance between Member States and

the exchange of information, was received in this Spanish Agency for Data Protection

(AEPD) a claim dated 07/17/2019, made by an interested party before the authority

of data protection of Slovenia (Information Commissioner). The transfer of this

claim to the AEPD is made in accordance with the provisions of article 56 of the



RGPD, taking into account its cross-border nature and that this Agency is competent

to act as the main controlling authority.

The aforementioned claim is made against the entity MIRACLIA, with registered office and

single establishment in Spain, in relation to the mobile application for Android

called “***APPLICATION.1”, which allows users to carry out pranks

telephone calls to third parties. The user selects a joke and a "victim", who is contacted

telephone by MIRACLIA from your own system through a hidden number

(prank call), making a recording of the conversation that is put to

disposition of the application user.

The claim reveals a possible violation of the regulations of

protection of personal data, considering that the interested party is not informed about the

recording of the prank call and there is no possibility for him to exercise the

right of deletion. It is also noted that the application itself describes the

conflicting elements.

The data processing that is carried out affects interested parties in various

Member states. According to the information included in the IMI System, in accordance

with the provisions of article 60 of the RGPD, they have declared themselves interested in this

procedure the control authorities of Belgium, Greece, Cyprus, Denmark, Saxony,

Norway, Sweden, France, Hungary, Poland, Berlin, Lower Saxony, Slovakia, Ireland and

Mecklenburg-Western Pomerania.

In view of the facts exposed, the General Subdirectorate of Data Inspection

proceeded to carry out actions for its clarification, under the powers of

investigation granted to the control authorities in article 57.1 of the RGPD:

. Dated 12/02/19 it is verified that through the link ***LINK.1, it can be changed

the country in which the application operates. Among these countries are both belonging to

to the European Union (Austria, Belgium, Germany, etc.) and outside it (China, United States

United States, Argentina, Brazil, South Korea, etc.). It is also found that the terms and

conditions of use of the service are written in Spanish, Italian, French, English and

German.

. On 12/03/2019 a new installation of the application is made, verifying that

In the process, it does not give the option to configure another country or another language, although the terms and

conditions of use of the service are written in Spanish, Italian, French, English and

German just like those that can be accessed on the Internet.

Through the acting inspection, the documents

called "Terms and conditions of use of the service" and "Privacy Policy". In

the latter indicates the following:

"1. INTRODUCTION

This privacy policy applies to information we may obtain from or about

you when you use the mobile application ***APPLICATION.1 (the “Mobile APP” or the “Service”)”.

“Miraclia does not collect data from the recipients of the pranks. Miraclia's activity is the

to provide a means of telecommunications so that the owner of the telephone that is downloaded



the app, choose a prank and record it, leaving the data related to the recipient of the call

stored in the user's own terminal without Miraclia keeping information about the

recipient's phone number. Miraclia provides a storage service in the

cloud of the client's audio files and at no time does it broadcast or share with

no one that information, since it is private information of the user of the application”.

Likewise, the aforementioned Inspection Services carried out a test consisting of

download the application on a mobile terminal. It is found that during the process of

installation the user receives the same text reproduced above about the non-collection

data of the recipients of the pranks and, among others, the following message:

“Read these legal Terms and Conditions in detail and press accept if you are over 18

years and you accept all of the stipulated. Otherwise, leave the application and

remove it from the terminal. Remember, in case you record a prank and spread it with your friends,

it is because you have requested permission from the person who has received the joke or they have given it to you.

You are solely responsible for this action."

Immediately after this text, a button is included with the indication

"Continue".

On the other hand, the Inspection Services recorded in their report the result

of the investigative actions that gave rise to the reference procedure and the

indicated with the number E/02003/2018, in which an operating test was carried out

of the system used by the claimed party.

EIGHTH: Considering the cross-border nature of this claim, dated

03/03/2020, a draft agreement to initiate the sanctioning procedure was issued, which was

subsequently transmitted (03/13/2020) through the IMI System to the control authorities

interested parties (they are outlined in said initial draft agreement, which was

duly notified to that entity on 03/12/2020), without any of them having

formulated objections to said project within four weeks of the consultation,

understanding, therefore, that there is agreement on it.

The complaint forwarded by the Slovenian data protection authority is

similar in its scope and object to those that gave rise to this sanctioning procedure,

all of them related to the mobile application for Android called

"***APPLICATION.1". For this reason, the draft initiation agreement transmitted to the

interested authorities through IMI, formalized for the sole purpose of completing the procedure

provided for in the RGPD and LOPDGDD (articles 60 and 64, respectively), collected the same

presumed infractions and the same amount of sanction that was fixed in the agreement of

opening of this procedure.

This being the case, and taking into account that this sanctioning procedure has

as object the analysis of the operation of the application of jokes "***APPLICATION.1",

from the point of view of the protection of personal data, globally considered, and not

the specific action of MIRACLIA in relation to specific claimants, is

understands that there is no formal opening of a new sanctioning procedure from

the complaint forwarded by the Slovenian data protection authority that could

give rise to a double sanction for the same infractions, for which it was agreed

incorporation to this sanctioning procedure, to resolve in a single act according to



proceed in law. Likewise, it was ordered that this procedure continue its processing

according to the cooperation mechanism contemplated in article 60 of the RGPD.

NINETH

: On 07/14/2020, by the General Subdirectorate of Data Inspection,

Access the information available on the MIRACLIA entity in “Axesor”. on said website

there is a turnover in the 2018 financial year, the last financial year presented, of 475,823

euros and a result for the year of -7,364 euros. Also, it is indicated that it is a

microenterprise, with 2 employees.

According to the information that appears in the Central Mercantile Registry, the "Subscribed Capital"

amounts to 6,000 euros

TENTH: On 07/24/2020, a resolution proposal was issued in the following sense:

1. That the Director of the AEPD sanction the entity MIRACLIA, for an infraction

of articles 13 and 14 of the RGPD, typified in article 83.5.b) and qualified as very

serious for prescription purposes in article 72.h) of the LOPDGDD, with a fine for

amount of 20,000 euros (twenty thousand euros).

2. That the Director of the AEPD sanction the entity MIRACLIA, for an infraction of article 6 of the RGPD, typified in article 83.5.a) and classified as very serious to effects of prescription in article 72.1.b) of the LOPDGDD, with a fine amounting to 20,000 euros (twenty thousand euros).

3. That the Director of the AEPD requires the MIRACLIA entity so that, within the term that is determined, adapts to the personal data protection regulations the operations of treatment that it carries out, the information offered to its clients and the procedure through which they must give their consent for the collection and treatment of your personal data, with the scope expressed in the Foundation of Law XI of the resolution proposal. Such adaptation must be implemented equally in all countries of the European Economic Area in which MIRACLIA operates through the application "***APPLICATION.1".

The aforementioned resolution proposal was notified to the MIRACLIA entity, dated 08/03/2020, this Agency received a letter of allegations in which it requests the file of actions based on the following considerations:

A. What MIRACLIA calls "Technical Facts":

MIRACLIA is a telecommunications company that operates a service called "***APPLICATION.1", which is subject to the regulation of "communications service interpersonal electronic communications based on numbering".

In this regard, it warns that the service "***APPLICATION.1" is in a scenario technical and data processing different from the one presented in previous actions of the Agency and Ordinary Justice. In fact, the scenario of the service in force on the dates of complaints is subject to the version of the service that has been audited by an engineer in collegiate telecommunications (provides a copy of the corresponding report) of which draw the following conclusions or "Final Opinion":

"1. The number-based interpersonal electronic communications service

“***APPLICATION.1” meets the attributes and characteristics defined in the Directive (EU)

2018/1972 establishing the European Electronic Communications Code

(CECE), which allow it to be classified as an electronic communications service

relationships based on numbering, as defined in article 2 (paragraphs 5 and

6) of the same.

2. The regulatory framework applicable to electronic communications services makes

a clear distinction between the production of content, which implies responsibility

editorial, and the transmission of content, which does not imply any responsibility

editorial (article 2 section 4 of the CECE and judgments of the Court of Justice

Fourth) of June 5, 2019 and June 13, 2019) of the Court of Justice of the

EU (CJEU).

3. The user of the interpersonal electronic communications service based on

numbering “***APPLICATION.1” (person who initiates the transmission) determines

unilaterally the recipient of the same, on which there is no condition whatsoever that

requires that you be a user of the “***APPLICATION.1” service but that you are a recipient

freely chosen by the former based on public numbering resources and on

whose data, public access and known by the user, is not processed

any “***APPLICATION.1”.

4. From the moment the electronic communications service begins

based on numbering, "***APPLICATION.1" is limited to facilitating the

physical means, own or third parties, for the transmission of the signal between who initiates

the transmission and the recipient of the same chosen by the latter, fulfilling the requirements

of quality, privacy, security and transparency included in the aforementioned directive.

5. “***APPLICATION.1” does not record the conversation. The recordings are

made by the user who has contracted the service of "***APPLICATION.1" (person

that initiates the transmission) in a private domain assigned exclusively to said

user (in the cloud by assigning a private URL) who, as part of

your right for your participation in editing them and by accepting the conditions

of use of “*** APPLICATION.1”, unilaterally decides to record them for personal use.

6. "*** APPLICATION.1" does not retain data of the final recipient except those that,

As a minimum, it allows you to comply with the provisions of the regulations on

data retention and provide the service to the user thereof. That is, the directive

2006/24/EC on the conservation of data generated or processed in relation to the

provision of electronic communications services, transposed in Spain by the

Law 25/2007.

7. “***APPLICATION.1” offers the possibility that persons or entities, which by

make use of networks hosted by public numbering resources can be chosen

as recipients of transmissions by users of “***APPLICATION.1”, may

request inclusion in a "black list" to inhibit the receipt of communications

electronically through the “***APPLICATION.1” service.

8. In accordance with the provisions of Considering 173 and Article 95 of the

RGPD, which establishes that said Regulation will not impose additional obligations on

natural or legal persons in terms of treatment within the framework of the provision of public services of electronic communications in public networks of communication in areas in which they are subject to specific obligations with the same objective established in Directive 2002/58/CE” (Directive on privacy and electronic communications). In this regard, it is worth bearing in mind established in Recital 34 of Directive 2002/58/EC: “It is necessary, therefore, regarding the identification of the originating line, protect the right of the interlocutor who makes the call to reserve the identification of the line from which he makes such call and the called party's right to reject calls from unidentified lines. Therefore, the right of the user who initiates the transmission (joker) of not presenting your telephone number to communicate it to the recipient, since, first, user and recipient make use of public resources of numbering and transmission is carried out through public communications networks electronic and, secondly, it is necessary, with regard to the identification of the line of origin, protect the right of the party making the call to reserve the identification of the line from which you make the call and the right of the caller called to reject calls coming from unidentified lines (Whereas 34 of Directive 2002/58/CE).

B. What MIRALCIA calls “Regulatory framework”:

1) At the service of number-based interpersonal communications (“***APPLICATION.1”), the considerations described in article 95 of the RGPD (“This Regulation will not impose additional obligations on people physical or legal in terms of treatment. within the framework of the provision of services of electronic communications in public communication networks of the Union in areas in which they are subject to specific obligations with the same objective established in Directive 2002/58/EC”).

2) MIRACLIA does not process the data at any time for the reasons

following:

a. These cases are outside the scope of regulation of the RGPD based on the

Considering 18 and article 2.2.c) of the RGPD, for referring to data processing

made by a natural person in the exercise of activities exclusively

personal or domestic.

b. The only person responsible for the treatment is the user of "***APPLICATION.1" and not

MIRACLIA. The user carries out the treatment directly because he is the person who,

freely, makes the necessary editing for the act of the prank (edits the prank to

to spend; enter the phone number of the overwhelmed person and press the call button;

decides whether to generate the file with the recording of the joke and, therefore, the URL of the

itself, which is personal and only known by the user). Furthermore, it is always his own

user who spreads the joke in his particular environment.

MIRACLIA only intervenes to provide the electronic communications service

interpersonal relationships based on numbering, which the user of the service has contracted.

Based on this, he proposes that the Agency go to the pranksters with the same action

sanctioning than against MIRACLIA.

c. During the whole process of the prank, the user of the application and responsible for the



treatment does not obtain any economic benefit, for which reason the

Considering 18 of the RGPD and article 2.2.c) cited.

3) Cite “examples” of other companies that provide electronic communications services

interpersonal relationships based on numbering and on which, according to MIRACLIA, the
The Spanish Data Protection Agency has not carried out any type of investigation or
inspection for similar reasons, in which the communications service provider
is never responsible (user of a telephone operator who calls an acquaintance and
Insults occur in communication; or who calls a public or private center to
warn about the existence of a bomb; a computer attack in which the virus uses the
communication networks and storage of digital information to infect other people;
use of an application to hold a videoconference meeting between subscribers
with public numbering, which allows the administrator to make a recording of it;
the interpersonal electronic communications service of “Burovoz” (***URL.1), which
allows its users to record telephone conversations between a user of the service and
another person, who is not a user of the "Burovoz" service, but has a telephone number
public numbering system phone. The operation of this service is
exactly the same as “***APPLICATION.1” and not only is it 100% legal but its
recordings have been and are totally valid when presenting them as evidence in a
judicial process in Spain.

4) On the subject of recordings of telephone calls made by users
of “*** APPLICATION.1”, Judgment No. 114/1984, of November 29, issued by the Chamber
Second of the Constitutional Court establishes that "Whoever records a conversation of other
attentive, regardless of any other consideration, to the right recognized in art.
18.3 CE; on the contrary, whoever records a conversation with another does not incur, for this only
fact, in conduct contrary to the aforementioned constitutional precept.”

5) Article 20 of the Spanish Constitution collects and protects the rights to: “To the
literary, artistic, scientific and technical production and creation.”, all of them framed within
of the right to freedom of expression held by all Spanish citizens in
general and the user of “***APPLICATION.1”.

6) In its final considerations, it adds that compliance with the withholding obligation

of data imposed by Law 25/2007 has allowed the entity to attend effectively and

within the times set by the RGPD to the rights of access, rectification and

cancellation that have been requested by multiple recipients of the pranks, as well as the Forces and

State Security Bodies for investigations of possible crimes.

C. In relation to the complaints outlined in the Background of this resolution, it indicates

the next:

1. The complaint filed by claimant 1 should not have been admitted for processing due to the following

reasons:

a) The claimant refers to an identity usurpation by a police officer.

b) The claimant did not contact MIRACLIA to request the exercise of the rights

ARCOPOL.

c) It is very likely that the claimant suffered a joke from some other service of the

competition, for which it requests the Agency to require the operators of



telecommunications the extract of calls received in the number of the abromado.

d) On 10/30/2018, the claimant received a letter from MIRACLIA stating

notified him that "*** APPLICATION.1" did not have any joke similar to the one in its catalog

described by him and he was asked to provide the URL of that recording for his

cancellation, if out of service “***APPLICATION.1”. The claimant did not provide this information, for

what is understood is that the exercise of rights was provided sufficiently.

e) We observe in the dossier of the file that the complainant provides a recording of

WhatsApp. However, "***APPLICATION.1" never sends the content of the

jokes, since these can only be heard in the user's own application.

In addition, the files of the recordings of the pranks that users can

download to your device have a filename that is nothing like the one you

provide as proof. With what can be deduced that there may have been an act of

modification and the test should be invalidated at that time.

f) It is the intention of this company to study the possibility of filing a criminal complaint

against this man for false accusation and damage to the honor of the company.

g) For all these reasons, and given that MIRACLIA has always agreed to settle the rights of

users, ask the Agency to file this matter since it responded to the request for

access to their data and considering that, with the information available, the joke did not start

from a user of “***APPLICATION.1”.

2. MIRACLIA also considers that the claim should also have been inadmissible

filed by claimant 2 for the following circumstances:

a) The annoyed person knows perfectly well the prankster person or persons, therefore

that he should have filed the lawsuit against them and not against MIRACLIA, which does not

treatment of data of the abromado.

b) It is false that the overwhelmed person received a call at 3:30 in the morning,

since none of the pranks in “***APPLICATION.1” can be held at that time

local. In addition, "***APPLICATION.1", as an electronic communications service

interpersonal calls based on numbering, never make calls to any recipient once

the joke has occurred, since that is something that can only be done by the user of the

app.

c) The claimant did not contact MIRACLIA to request the exercise of the

ARCOPOL rights.

d) It is also false that once the access right “***APPLICATION.1” has been exercised

continue sending emails. “***APPLICATION.1” has never committed such practices nor the

commit.

D. Regarding the proven facts, MIRACLIA makes the following considerations:

There is a website with

. Proven Fact 1: MIRACLIA owns an electronic communications service

number-based interpersonal relationships accessed through an application

named “***APPLICATION.1”.

same name,

“***APPLICATION.1”, as a commercial information and user service that does not

is part of the electronic communications service provided by MIRACLIA nor has it been

object of complaint.

. Proven Fact 2: By virtue of the provisions of article 95 of the RGPD, users are not required to

interpersonal electronic communications services based on public resources of

numbering that identifies the manager of the call or the owner of the platform or that

indicate where to obtain information on the call or on the exercise of rights. What



it has been said “***APPLICATION.1” is an application to access a service of

interpersonal electronic communications, reserving the user of the same the right

or not to personally identify and record said call.

. Proven Fact 4: The reference to hosting the pranks on a public site is

wrong. Access to the audio is via a token-based URL as

used in thousands of private access websites (eg, the package tracking website of a

courier service or multitude of public services for the payment of fines). The URL to

that the inspector mentions is generated automatically on the server, so that when

not be a fixed or static URL can only be accessible by the user of the service

interpersonal electronic communications based on public resources whose name is

“***APPLICATION.1”. Only the sender of the joke and the recipient have access to said URL.

of the same if the emitter of the joke wants to do it (it is his responsibility).

. Proven Fact 5: in this proven fact it is indicated that through the link

***LINK.1, you can change the country in which the application operates. However, it

unknown how the Agency has accessed that pre-production platform that is a

test prototype that has never worked in production and therefore has never

could be used by an end user as an electronic communications system. The

The purpose of said prototype was to offer the electronic communications service in

multi-platform mode such as Skype, for example, which can be used with an app or

on a computer regardless of its Operating System.

. Proven Fact 9: No joke appears in any catalog of MIRACLIA jokes

supplanting any organization or person, much less the Police. There are multitudes of

other prank services that in addition to copying MIRACLIA's catalog, are likely to

They have introduced one that supplants the Police, but MIRACLIA does not know it.

E. In response to the considerations set forth in Legal Basis IV, referred to

to the definition of data processing of a personal or domestic nature, MIRACLIA performs

the following statements:

. Is personal or domestic the conversation that takes place for the provision of a service of

number-based interpersonal electronic communications. The data from

numbering are public resources on which an operator does not process. The

user of said service and on which treatment is done is who registers in the

itself and chooses the recipient of the call based on these public resources. It is said

user who records the call using complementary tools to the service

basic electronic communications. The CJEU references cited do not refer to the

case of this type of services.

In addition, it is the user who decides freely and sovereignly who directs the prank

within your known contacts or family or friends.

. It is not valid for "*** APPLICATION.1" the declaration of the Court of Justice on the aforementioned

concept, contained in the Judgment of 07/10/2018, according to which "it will not proceed to consider

that an activity is exclusively personal or domestic when its purpose is to allow

to an undetermined number of people access to personal data or when the activity

extends, even in part, to the public space and is therefore directed towards the

outside the private sphere of the person processing the data". The

object of the service is to establish an electronic communication initiated by the prankster,

who decides to record her and have access to her private recording. Sharing it in your circle

private is the decision of the prankster, who in the T&C is warned that he can break rules

regulations according to the treatment you make of that data (yours private). The object of



service is in no case the indiscriminate sharing of the recording.

. The proposal indicates that "MIRACLIA's action is essential given that, without its

contest it would not be possible to process data since it is carried out in the process.

MIRACLIA facilitates the means to make the call, facilitates the means to choose a prank, and

it provides the means to record and store a joke." In this regard, MIRACLIA affirms that

it is logical that it be this way, since you have defined "***APPLICATION.1" as a

number-based interpersonal electronic communications service with that

functionality and must be governed in everything related to it as described by the standards of

current regulation (Directive (EU) 2018 / 1972 establishing the European Code of

Electronic Communications (CECE), as defined in article 2, sections 5 and 6, of the

same.

F. The constitutional principle by the fact itself

“This principle has been called “personal responsibility”, which implies that only

a person can be held responsible for their own actions, that is, not to a thing

not even an animal.”

***URL.2

Following this principle and delving into what concerns us helps us to demonstrate that

***APPLICATION.1” as an interpersonal electronic communications service based on

in numbering cannot bear any responsibility for the act committed by the

user of “*** APPLICATION.1”, in the same way that you can never request

liability to a gun manufacturer for the act committed by a person doing

misuse of said gun.

G. Other final considerations

. That the URLs that can be received by the pranksters, once the

call recording, they are NOT public URLs. The URLs generated by the server software

for the user of “***APPLICATION.1” are private and cannot be indexed by users.

Search engine spiders, such as Google, Bing or Yahoo.

. That the Agency take into account File No.: TD/00007/2017, in which the

case of a person overwhelmed by the Radio4G station and the broadcast live and to the entire

radio4G audience and that ends up in the file of the performances.

. Everything stated in this writing is endorsed both in the technical audit that is now

is in the visa phase by the COIT (Official College of Engineers of

Telecommunications) as in the conditions of use that the user accepts before being able to

use the platform.

Finally, request a face-to-face hearing procedure to clarify before the

instructors / inspectors of the Agency the exposed points and warns that, in case of not

see their interests served, reserves the right to go to other higher instances

and/or judicial in Spain and in Europe.

With your brief of allegations, you provide a copy of the report corresponding to the audit

referred technique, carried out by a telecommunications engineer on 07/29/2020.



This report is structured in four sections:

. Objectives and methodology of the work.

. Description of the service “***APPLICATION.1”

. Audit results

. Final opinion.

As indicated, it is based on personal interviews, practical tests of execution of

“***APPLICATION.1” on two mobile devices and the tests of the application tools

editing, recording and metadata of the content of the messages, although it does not provide details

on the development of these tests, limiting itself to listing a series of findings.

The following is indicated in the “Results of the Audit” section:

“Regarding the specific analysis of the service “*** APPLICATION.1” it has been possible to

verify the following facts:

a) Only a user registered in the service can start the conversation

“***APPLICATION.1”.

b) The user of the service “***APPLICATION.1” is the only one involved in the process that

you can freely determine the recipient of the conversation

c) To determine the addressee of the conversation, resources of

public numbering.

d) It is not required, nor is such a circumstance verified or proven by any means, that the

recipient of the conversation is a user of the “***APPLICATION.1” service.

e) Once the connection is established between the user of “***APPLICATION.1” and the recipient

of the conversation allows the direct exchange of interpersonal information through

of electronic communications networks between both people.

f) “***APPLICATION.1” offers the user who contracts said service a set of templates

preconfigured for editing a voice message.

g) The user who contracts the service "***APPLICATION.1" is the one who freely chooses between the

themselves to determine the content of the message to be transmitted.

h) The recording is made in a personal and private domain assigned exclusively to the

user of the service “***APPLICATION.1” (person who initiates the transmission), as a service

that lends “***APPLICATION.1” to the user in the cloud on their own premises.

i) The recording domain offered by “***APPLICATION.1” to the user of said service is

a private and secure domain.

j) The final decision on whether or not to record the message on your domain

private falls exclusively on the user of the service "***APPLICATION.1".

k) “***APPLICATION.1” offers the user who contracts said service a set of

interactive metadata tools to carry out possible actions on the

edited message.

l) “***APPLICATION.1” offers any person or entity that is part of a

use of public numbering resources the possibility of joining “black lists”, to

stop receiving calls from users of “***APPLICATION.1”.

m) In fact, certain numbers of the public numbering plan are included by

defect in said “black list” (091, 061, 112, 092, etc.).

n) “*** APPLICATION.1” facilitates the physical means, own or third parties, for the transmission

of the signal between who initiates the transmission and the recipient of the same that you have chosen.

o) "*** APPLICATION.1" does not retain data of the final recipient except those that, with

character of minimums, allows you to comply with the provisions of the regulations on retention of



data".

In the section above the one indicated, the label as "Description of the service

***APPLICATION.1”, the information provided by MIRACLIA to the auditor engineer is summarized,

which literally coincides with the "facts" that are detailed as a result of the audit.

The aforementioned report includes an Annex II, related to the "Initial premises and regulations

reference". This Annex refers to the definition of communication service

interpersonal electronics introduced by the European Electronic Communications Code

(CECE), which are those that allow the exchange of interpersonal information and

interactively through electronic communication networks between a finite number of

people, in which the people who initiate or participate in the communication determine their

recipients, and add the following:

“In the conditions of use of the application ***APPLICATION.1 in article 6 it is indicated that

“As with any telecommunications service, it is illegal to use the services of

***APPLICATION.1 for the purpose of harassing or harming anyone.” There is therefore a

contractual declaration that ***APPLICATION.1 is a service subject to the regulation of

telecommunications and, therefore, an implicit acknowledgment that it is a service of

electronic communications in such a case.

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

Data in this procedure are considered the following,

PROVEN FACTS

1. The MIRACLIA entity is the owner of the mobile application and web service called

“***APPLICATION.1”. This application allows users to perform pranks

telephone calls to third parties. The user selects a joke and a "victim", who is contacted

telephone by MIRACLIA from your own system through a hidden number

(prank call), making a recording of the conversation that is put to

disposition of the application user.

The use of the mobile application and web services mentioned is regulated in the document called

"Terms and Conditions of Use of the Service", which is declared reproduced in this act to

probative effects. The content of this document includes the following:

<<By using the Service, you will be bound by the Terms of Use and the Privacy Policy

Privacy, expressly accepting its compliance and entering into force a legal contract

binding on us…if you do not agree to these Terms of Use and/or

Privacy Policy We recommend that you uninstall the application from your terminal.

3. Service definition

***APPLICATION.1 is an application that allows the user to send jokes consisting of

a pre-recorded audio file via telephone to the destination selected by the user. The

The user will be able to select from a list of jokes and indicate both the destination line

such as the time you want the recipient to receive the prank. Once the

joke, the application has the functionality to share and record the audio file (in

forward the "Recording"), notwithstanding which, it will be an essential requirement that the user

have the express consent of the person who has received the joke to be able to

obtain it and then make use of it.

(…)

NOTE: Since the personal data of the recipient of the call is stored

solely and exclusively in the terminal of the user of the application (client), in the event that

he deletes the application on his terminal or deletes the data associated with it on his terminal,

it may stop working in the sense that the deleted information disappears from the

same.

(…)

5. Payment services

The use of the application may incur a cost...

The amounts purchased will expire after 6 months without using the application. At that moment,

user content may be removed.

6. Use of the services offered

Through these Terms and Conditions of Use of the Service, the User contracts

with MIRACLIA a leisure and entertainment service that allows the User to send jokes

phone calls to a recipient and then play, download, or share the prank.

With the acceptance of these Terms and Conditions of Use of the Service, the User

of ***APPLICATION.1 assumes the following responsibilities:

(…)

b) Share and record pranks

The User, as the owner of the recording, is fully responsible for obtaining the

express and unequivocal consent of the person who has received the joke, for the

recording and broadcasting.

The laws allow the recording of any telephone conversation as long as it is counted.

with the consent of at least one of the two parties involved in it. A

user may not download a Recording without obtaining the prior consent of the

recipient of it. The operation of the Service prevents the generation of a

Recording if the user of ***APPLICATION.1 does not expressly accept such prior condition.

In order to share jokes publicly, the Service requires that the person

shares the joke has obtained permission to do so from all participants in the

call. MIRACLIA is not responsible for the consequences of non-compliance with the

Obtaining the necessary consents to share the Recording, falling on

him the obligation to indemnify third parties or MIRACLIA from any claim arising

of their actions.

(…)

8. Limitation of liability

MIRACLIA responsibilities:

MIRACLIA acts only as an intermediary between the sender and the receiver of the prank.

MIRACLIA does not decide at any time on the purpose, content and use of the treatment

of the recording and, therefore, cannot be held responsible for it.

(…)

If the recipient of the joke (as the owner of the data and exercising their right to object or

cancellation) or the sender of the prank (as the owner of the recording) request

MIRACLIA cancellation of the recording, automatically the recording is removed from the

servers that provide service to MIRACLIA.

However, prior to the exercise of the right of opposition or cancellation by the

receiver, the prank could have been downloaded to the User's device, being already



said recording outside the scope of MIRACLIA and, therefore, the entity is not

responsible for the use, disclosure, modification that the User makes of it.

(…)

9. Data protection

We have established a Privacy Policy to explain how we collect and use

information about you (the user)…>>.

2. The Inspection Services of the Agency, dated September 6, 9 and 12, 2019,

carried out tests consisting of downloading the application on a mobile terminal and

proceed to its use by arranging for prank calls to be made. As a result of

The following findings were obtained from these actions:

. During the installation process, the user receives, among others, the following messages:

“Read these legal Terms and Conditions in detail and press accept if you are over 18

years and you accept all of the stipulated. Otherwise, leave the application and

remove it from the terminal. Remember, in case you record a prank and spread it with your friends,

it is because you have requested permission from the person who has received the joke and they have given it to you.

You are solely responsible for this action.”

“Miraclia does not collect data from the recipients of the pranks. Miraclia's activity is the

to provide a means of telecommunications so that the owner of the telephone that is downloaded

the app, choose a prank and record it, leaving the data related to the recipient of the call

stored in the user's own terminal without Miraclia keeping information about the

recipient's phone number. Miraclia provides a storage service in the

cloud of the client's audio files and at no time does it broadcast or share with

no one that information, since it is private information of the user of the application" (this

paragraph is also included in the privacy policy).

Immediately after these texts, a button with the indication "Continue" is included.

. The application "***APPLICATION.1" consists of 3 tabs: "List" (jokes available),

"Examples" and "My jokes". In this last tab the pranks made by

the joker, if they are not eliminated.

. The phone number of the incoming prank call appears as "Private Number" in

all cases.

. In the version installed for testing, the latest available in the app store

for Android operating systems "Play Store", the joker, has no option to choose whether the

joke is recorded or not. The joke is always recorded, unless the receiver

decide to delete it following any of the procedures established for it. If this doesn't

occurs, the recording remains in MIRACLIA's systems until the prankster decides

eliminate it or, as a general rule, for a period of time of 6 months after the use of

the application, established by the entity itself.

. At no time throughout the phone conversation is the application identified

***APPLICATION.1 as manager of the call nor to the developer company MIRACLIA

as the owner of the platform. Therefore, the receiver of the prank does not know where

You should go to get more information about the call or exercise your rights.

. At no time is the joker quoted.

. Nor is it reported at any time, during the development of the joke, that the

conversation is being or may be recorded.

. It is verified that at the end of the joke the following locution is heard: "A friend of yours

he played a joke. In case you don't want your friend to be able to listen, download

or spread the joke, or in case you don't want to receive any more jokes, press 5 with your keyboard

after the signal. beep”

From the end of the joke until the locution occurs, a space of

silent time of 10 seconds.

. The “deletion” of the prank recording and the inability to continue receiving pranks

pressing key 5 once the signal indicated in the final announcement has been heard, it has been unstable

in the tests carried out. On one occasion when the 5 key was pressed before the signal and

another later, the mechanism failed; on two other occasions when it was pressed only once

after the signal, it was removed successfully. It was found that there is no confirmation

deletion of the prank, simply, when approximately 10 seconds elapse

from the indicated signal to press the key 5, the communication is cut off.

In cases where the deletion worked correctly, the prank disappears from the list

of pranks made by the prankster, therefore not being able to be shared, downloaded or

heard. It has also been verified that the telephone number was blocked for the

receiving more jokes.

. In the list of pranks made by the prankster, next to each of the pranks not

eliminated by the receiver of the prank following the indicated procedure, three

icons: one to download the audio file of the recording of the telephone conversation

of the joke, another to listen to it and a third to share it. In the latter case, it

send the link to the audio file of the recording through the chosen medium

to share it. This is the only time the prankster knows the link to the file

audio.

. In the event that the prankster leaves his finger pressed on a certain prank in the

list of pranks performed, a pop-up window appears offering the possibility of

remove the audio file from MIRACLIA systems, but this action is not as

intuitive like the previous three as it lacks a specific icon.

. In the saved pranks, there is the destination phone number, type of prank, date and

completion time.

. Uninstalled the application and reinstalled again, it is observed that the phone numbers

of the pranks made appear as “?????????”, which suggests that

this data is stored locally, and not on MIRACLIA's servers.

. Prank calls can be instant or scheduled by specifying date and time.

execution time. In this case, the recipient's phone is stored in the

the MIRACLIA entity until the moment of making the call. In this regard, MIRACLIA



has declared in his allegations that the telephone number of the recipient of the prank remains

queued with the call to make, which disappears from your systems when the call

is done.

The acting inspector scheduled a prank on his terminal for deferred execution and

then said terminal was turned off. The call was made at the scheduled time,

which turns out that the phone was stored in the MIRACLIA systems until

time to run the prank (minutes, hours, days or months)

. For the suppression of the recording there are only two options: that the prankster follows the

deletion procedure described from the application; or request it from MIRACLIA,

difficult issue for the affected considering that it is not shown in any

moment who manages the call, nor the company responsible for it. Also, for

The affected person will need to know the link to the audio file and does not have this either.

information, unless provided by the user (the joke can be eliminated by knowing the

url of the recording and using the mechanism enabled on the web together with the request for

telephone line number blocking).

3. MIRACLIA offers on its website "***APLICACIÓN.1.es" a free and immediate system for

include a phone number in the list of blocked phones.

Through the current inspection, a test was carried out, registering in said system the number

telephone number corresponding to the second SIM of the acting inspector's terminal.

Subsequently, a prank was attempted on that phone number and the application did not

allowed his execution.

4. MIRACLIA does not have a platform where the jokes made are published

so that any third party can access, but the recordings of the pranks are

are housed in a public site, which enables access to them through the

link to the audio file, which can be broadcast indiscriminately by the user

joker.

5. On 12/02/19 it is verified that through the link ***LINK.1, you can change

the country in which the application operates. Among these countries are both belonging to

to the European Union (Austria, Belgium, Germany, etc.) and outside it (China, United States

United States, Argentina, Brazil, South Korea, etc.). It is also found that the terms and

conditions of use of the service are written in Spanish, Italian, French, English and

German.

6. On 12/03/2019, an installation of the application is carried out, verifying that the

process does not give the option to configure another country or another language, although the terms and conditions

of use of the service are written in Spanish, Italian, French, English and German, the

same languages that are available when accessing the web over the Internet.

7. Claimant 1 has stated that, on ***DATE.1, he received on his line of

mobile phone ***PHONE.1 a prank call through the application

“***APPLICATION.1”, in which a person pretended to be a police officer. He denounces that the

call was recorded and broadcast to third parties without your knowledge or consent; and that the

call occurs from a hidden number.



8. Claimant 2 has stated that, on ***DATE.2, she was the subject of a call

phone prank carried out using the application "***APPLICATION.1", which was

recorded and disseminated on social networks with the mention of his name without his permission (provides

the link to the audio object of the complaint “***LINK.1”)

On 08/26/2019, the Inspection Services accessed the website

“***APLICACIÓN.1.es”, to the URL corresponding to the recording of the joke made to the

claimant 2. It is verified that using the right button shows different

options, including playing and downloading the recording.

9. The Agency's Inspection Services have verified that the reported pranks

by claimants 1 and 2 are listed in the prank catalog of available at

“***APPLICATION.1”.

FOUNDATIONS OF LAW

Yo

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

Control, and according to what is established in articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection is competent to resolve this

process.

Article 63.2 of the LOPDGDD determines that: "The procedures processed by

The Spanish Agency for Data Protection will be governed by the provisions of the Regulation

(EU) 2016/679, in this organic law, by the regulatory provisions issued

in its development and, as long as they are not contradicted, on a subsidiary basis, by the rules

general administrative procedures."

II

Article 56.1 of the RGPD, regarding the "Competence of the supervisory authority

main", states the following:

"1. Without prejudice to the provisions of article 55, the supervisory authority of the main establishment

or of the only establishment of the person in charge or of the person in charge of the treatment will be competent to

act as the lead supervisory authority for cross-border processing carried out by

said person in charge or person in charge in accordance with the procedure established in article 60".

Said article 60 regulates the "Cooperation between the main control authority and the

other interested control authorities":

"1. The main control authority will cooperate with the other control authorities concerned

agreement with this article, striving to reach a consensus. control authority

principal and the control authorities concerned shall exchange any relevant information.

2. The main control authority may at any time request other authorities of

Control interested parties that provide mutual assistance in accordance with article 61, and may carry out

joint operations under Article 62, in particular to conduct investigations or

supervising the application of a measure relating to a controller or a processor

established in another Member State.

3. The main control authority shall promptly notify the other control authorities
relevant information in this regard. It shall promptly transmit a draft decision
to the other interested control authorities to obtain their opinion on the matter and will have
due account of their views.

4. In the event that any of the interested control authorities raises an objection
relevant and reasoned information on the draft decision within four weeks of the
consultation in accordance with paragraph 3 of this article, the main supervisory authority shall submit the
matter, in the event that it does not follow what is indicated in the pertinent and motivated objection or considers that said
objection is not relevant or is not motivated, to the coherence mechanism contemplated in article
63.

5. In the event that the main supervisory authority plans to follow what is indicated in the relevant objection
and motivated received, it will present to the opinion of the other interested control authorities a
revised draft decision. This revised draft decision will be submitted to the procedure
indicated in section 4 within a period of two weeks.

6. In the event that no other interested supervisory authority has objected to the
draft decision transmitted by the main supervisory authority within the period indicated in the
paragraphs 4 and 5, it will be considered that the main control authority and the control authorities
Stakeholders agree to and are bound by that draft decision.

7. The main control authority shall adopt and notify the decision to the main establishment or to the
sole establishment of the person in charge or the person in charge of the treatment, as appropriate, and will inform
the decision to the control authorities concerned and to the Committee, including a summary of the
pertinent facts and motivation. The supervisory authority to which a complaint has been filed

claim will inform the claimant of the decision.

(…)

12. The main control authority and the other interested control authorities will be provided reciprocally the information required within the framework of this article by electronic means, using a standardized form.

On the issues regulated in these precepts, what is indicated is taken into account in Recitals 124, 125, 126 and 130 of the RGPD.

In accordance with the provisions of the previous regulations, in the present course, referring, among others, to a claim filed with the control authority of a Member State (Slovenia), in relation to processing in the context of activities of a single establishment of a controller that affect or are likely to substantially affect data subjects in more than one Member State (data processing cross-border), the main control authority, in this case the Spanish Agency for Data Protection, is obliged to cooperate with the other interested authorities.

The Spanish Agency for Data Protection, in application of the powers that conferred by the RGPD, is competent to adopt the decisions designed to produce legal effects, whether it is the imposition of measures that guarantee compliance with the regulations or the imposition of administrative fines. However, it is required to involve closely and coordinate the control authorities interested in the decision-making process decision-making and take their opinion into account to the fullest extent. It is also established that the binding decision to be adopted is jointly agreed upon.

Article 60 of the RGPD regulates this cooperation between the control authority principal and the other control authorities concerned. Section 3 of this article expressly establishes that the main supervisory authority will transmit to the other control authorities concerned, without delay, a draft decision to obtain their opinion on the matter and will duly take into account their points of view, following for

this the procedure provided for in sections 4 and following. Control authorities



interested parties have a period of four weeks to formulate reasoned objections

about the draft decision, it being understood that there is agreement on said draft if

no authority submits objections within the indicated period, in which case all of them

are bound by the repeated project.

The aforementioned article 60, paragraph 12, provides that the main supervisory authority and the

other interested control authorities will reciprocally provide each other with the information

required within the framework of this article by electronic means. It is up to do it

through the “Internal Market Information System” (IMI System).

On the other hand, article 58.4 of the RGPD establishes that the exercise of powers

conferred on the control authority must respect the procedural guarantees established in

the law of the Union and of the Member States.

The Spanish procedural regulations, specifically, Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (LPACAP), establishes

that sanctioning procedures will always be initiated ex officio by

agreement of the competent body, which must contain, among other indications, the

identification of the person or persons allegedly responsible, the facts that

motivate the initiation of the procedure, its possible qualification and the sanctions that could

correspond

In accordance with the rules expressed above, considering the nature

cross-border of this claim, dated 03/03/2020, a draft agreement was issued

start of sanctioning procedure, which was later transmitted through the System

IMI to the interested control authorities, which are listed in the background,

without any of them raising objections to said project within four

weeks from the consultation, understanding, therefore, that there was agreement on it.

On the other hand, section 4 of the aforementioned article 64 of the LOPDGDD establishes that

The processing times established in this article will be automatically

suspended when it is necessary to collect information, consultation, request for assistance or

mandatory pronouncement of a body or agency of the European Union or of one or more

several control authorities of the Member States in accordance with the provisions of the

RGPD, for the time between the request and the notification of the pronouncement to the

Spanish Data Protection Agency.

III

This procedure is initiated by virtue of the claims received in this

Agency against the entity MIRACLIA, in which those affected (overwhelmed) denounce the

use of your personal data to make a joke using for it the

application "***APPLICATION.1", by means of a telephone call to their mobile telephony lines.

The recording made of the call without the knowledge of those affected and the

dissemination of said recording to third parties, also without your consent.

The procedure, therefore, aims at the global analysis of the application

"***APPLICATION.1" from the point of view of data protection regulations

personal and in relation to the people receiving the prank calls.

Any analysis of the position of the users of the application is omitted

(pranksters), as well as the information that MIRACLIA offers to them and the

treatment of your personal data.

In accordance with the foregoing, the conclusions that could be derived from this

procedure will not imply any pronouncement regarding the previous aspects

discarded.

IV

Previously, it is appropriate to consider the allegation made by MIRACLIA in

relation to the position he occupies, in his opinion, in the personal relationship between joker and

overwhelmed. The aforementioned entity considers that its intervention is limited to providing a means of

leisure between individuals, which acts as an intermediary in a relationship between individuals.

In accordance with this approach, MIRACLIA understands that the regulations of

protection of personal data is not applicable to this case, because spending a

joke through an application or a medium in which the user is sovereign of the

information that is provided is an act developed in the domestic or personal sphere and, therefore,

therefore, excluded from the scope of protection of said regulations as established in the

article 2.2 of the RGPD and article 2.2.a) of the LOPDGDD. It says to article 2.2 of the RGPD:

"two. This Regulation does not apply to the processing of personal data:

c) carried out by a natural person in the exercise of exclusively personal activities or

domestic".

This Agency, on the other hand, considers that the actions of the entity complained against

can be included in this exception for three reasons:

. MIRACLIA is not a natural person: article 2.2.c) of the RGPD, when establishing the exception

indicated, expressly refers to the processing of personal data carried out by a

Physical person.

. Your activity is carried out in connection with a professional or commercial activity. I know

constituted as a limited company, for profit and commercial nature.

. The RGPD applies in full to those responsible or in charge of the treatment that

provide the means to process personal data related to activities

personal or domestic (if indeed it was).

On these issues, recital (18) of the GDPR states the following:

“This Regulation does not apply to the processing of personal data by a person

physical activity in the course of an exclusively personal or domestic activity and, therefore, without connection

some with a professional or commercial activity. Personal or domestic activities include

include correspondence and keeping an address book, or activity on networks

social networks and online activity carried out in the context of said activities. However, the

This Regulation applies to those responsible or in charge of the treatment that provide the

means to process personal data related to such personal or domestic activities”.

We are facing business activities, with a business model based on

in carrying out pranks through an application in exchange for a price.



In order to define what should be considered treatment of an exclusively

personal or domestic, although in this case the application of those

precepts without entering into that analysis, it is convenient to take into account the

CJEU doctrine stated in the Lindqvist, Rynes and Jehovah's Witnesses judgments

(STJUE of July 10, 2018, C-25/17).

In accordance with these rulings, it can be considered that the CJEU understands, with

general character, that the exception of activities of an exclusively personal or

domestic must be interpreted in a strict sense, only when the processing of data
"incidentally" affects the private life or intimacy of "other people", other than the
responsible for processing personal data. It is also said by the Court that the
character of personal or domestic activities is not defined exclusively by opposition
to the dissemination of data, as MIRACLIA seems to indicate, but rather that this dissemination implies that
a treatment of personal data related to the private or family life of individuals does not
may be considered excluded from the protective regulations, so there may be other
cases in which even treating personal data of a personal or domestic nature, this does not
could be understood as included within the exception provided for in article 2.2 c) of the RGPD.
It is not possible to lose sight of the processing of personal data that is carried out in
the present case: it consists of a telephone call, to a telephone of a third person,
whose voice, when answering the call, is recorded in MIRACLIA's technical system.
As can be seen, in this case it is not that the privacy or intimacy of other people
is "incidentally" affected, but the very purpose of this data processing is,
precisely, the voice of the third person who is called. That is, the treatment of
personal data of the third party called is not a mere "incidental" annoyance within
a more general data treatment, but that the use of your personal data is
precisely the goal of treatment. Therefore, it cannot be considered in any case that
said data processing of the voice of the overwhelmed is merely incidental, but is
It is a “main” treatment.
The STJUE of July 10, 2018, C-25/17, Jehovah's Witnesses, establishes a
interpretation about the concept of exclusively personal or domestic activities
and it says like this:
42 As the Court of Justice has held, Article 3(2), second indent, of Directive
95/46 must be interpreted in the sense that it contemplates only the activities that are registered
within the framework of the private or family life of individuals. In this regard, it will not be appropriate to consider

that an activity is exclusively personal or domestic, for the purposes of said precept, when is intended to allow an indeterminate number of people access to personal data or when the activity extends, even in part, to the public space and is therefore directed outside the private sphere of the person processing the data (see, in this sense, the judgments of November 6, 2003, Lindqvist, C-101/01, EU:C:2003:596, section 47; of December 16, 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 44, and of December 11, 2014, Ryneš, C-212/13, EU:C:2014:2428, paragraphs 31 and 33).

In the case of MIRACLIA, it turns out that the "overwhelmed" natural persons transfer information to said entity, since the voice of the overwhelmed person is recorded in the application proportionate, and likewise those who are going to be pranksters also transmit it to MIRACLIA, because they provide you with the recipient telephone numbers of the calls you will make said entity. This telephone number is registered in the entity's systems until the completion of



the call, the conversation is recorded for the purpose of providing a content service multimedia that is accessed through mobile devices, offering the possibility to play, download and share the audio file. This means first of all that such activity is directed outside the prankster's personal and private sphere, into the interpretation of the CJEU, which excludes it in any case the exception "exclusively personal and private.

It follows that natural persons "pranksters" would transmit personal data to MIRACLIA, which registers (that is, "treats" said data) by recording them. But MIRACLIA

also "treats" in its systems the telephone number of said third parties,

potentially (when not materially) being able to establish a link between a

a certain phone number and a certain voice recorded on their systems. Namely,

MIRACLIA carries out personal data processing to which it cannot be applied in any

case the exception to which we refer.

But, in addition, although initially there is no link between MIRACLIA and

the "victim", a data processing consisting of a record of the

people who don't want to be teased anymore.

MIRACLIA's performance is essential given that, without its help, it would not be possible to

data processing carried out in the process. MIRACLIA facilitates the means to make the

call, provide the means to choose a prank, and provide the means to record and store

a joke, which means that it determines the treatment means and ends, organizes,

encourages and coordinates the activities of pranksters through your application

***APPLICATION.1, and thus participates, together with the pranksters, in determining the

purpose and means of the processing of personal data of the affected.

In addition, MIRACLIA, "attending to its own objectives" (commercial) influences the

pranksters and encourages it, so it must be held responsible,

together with the pranksters, of the data processing that is carried out by the

overwhelmed people.

v

Another of the preliminary issues raised by MIRACLIA has to do with the

existence or not of personal data. Questions that the information can be considered data

personal, since MIRACLIA is unable to identify the overwhelmed in a

simple and without disproportionate means, and points out that the only one who can identify the

overwhelmed is the user, who is anonymous to the entity.

He adds that he is not able to identify the overwhelmed person or link him to any other

data and that the voice is not personal data if it does not allow its owner to be identified or if it is

disproportionate efforts are required to identify it.

The RGPD defines the concept of “personal data” in its art. 4.1) as: “all

information about an identified or identifiable natural person ("the data subject"); I know

An identifiable natural person is considered to be 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

various elements of physical, physiological, genetic, psychic, economic,



cultural or social status of that person.

In accordance with these definitions, information relating to persons

recipients of the jokes that are carried out using the application

"***APPLICATION.1" collected by the MIRACLIA entity conforms to the definition of data

personal. In addition to the telephone number, MIRACLIA proceeds to also record the voice

of the people harassed through the opportune recording of the prank, susceptible to

be disseminated, in addition to other user data.

In relation to voice recording, Report 497/2007 of the Legal Office of

this Agency affirms that “sound recordings will allow the identification of a person,

even more so if that recording is attached to a file and therefore will be included in the file.

scope of application of the LOPD”. In the same sense, the Court has declared

National.

To the latter, add that the ruling of the National High Court dated 03/19/2014

(rec.176/2012) says that "the voice of a person constitutes personal data, as

as can be deduced from the definition offered by article 3.a) of the LOPD, as

<<any information concerning identified or identifiable natural persons>>,

This is a non-controversial question".

This is a broad concept that can include objective information, such as

It can be, for example, the name and surnames, or subjective information, such as

be the assessment of an examiner in a professional examination. The CJEU has understood this,

for example, in the STJUE of December 20, 2017, C-434/16, Peter Nowak.

That the RGPD considers the voice as personal data is undeniable. The opinion

4/2007, of June 20, 2007, on the concept of personal data (WP136), of the Group of

art work 29, likewise collects it, with examples. In example 2, on Banking

telephone, says: "In telephone banking operations, in which the voice of the customer who

gives instructions to the bank is recorded on a tape, the recorded instructions must be

considered as personal data. In the same way, both this Opinion 4/2007, and

Opinion 3/2012 on the evolution of biometric technologies (WP193) establish

that the voice can be both personal data, raw, and also used with techniques

biometrics

So that this acoustic characteristic of the human person can be considered

personal data, the RGPD determines that said information must refer to a person

identified or identifiable physical person, and considers an identifiable person to be one whose identity

can be determined, directly or indirectly through said personal data.

MIRACLIA starts from an erroneous premise, which consists in considering that

We are dealing with personal data because the MIRACLIA entity itself could not identify the

person whose voice is recorded (i.e., the "interested", the overwhelmed) since it does not store

the recipient's number.

This argument is wrong. The data protection regulations (Considering 26

of the RGPD) starts from the basis of a comprehensive protection of the fundamental right of

protection of data of the natural person, therefore, as we have already reasoned above,

exceptions must be interpreted strictly and the concept of data



broad-minded staff.

Recital 26 of the RGPD, in the part that is of interest now, reads as follows:

“The principles of data protection should apply to all information relating to a person

identified or identifiable physical Pseudonymized personal data, which could be attributed to a

natural person through the use of additional information, should be considered information about

an identifiable natural person. To determine whether a natural person is identifiable, one must take into account

taking into account all means, such as singularization, that can reasonably be used by the

responsible for the treatment or any other person to identify directly or indirectly the

Physical person".

As can be seen, the GDPR considers a person to be identifiable

when said person can be identified either by (i) the data controller, or

good by (ii) any other person.

As we have seen before, the “joker” could be considered as responsible

treatment together with MIRACLIA, so that being so, there is no doubt that the

Prankster can identify the voice of the person receiving the prank call. But,

Even if the prankster is not considered responsible for the treatment, it would be

considered as a "third party other than the person in charge", and the RGPD considers, even

in that case, that the "prankster" is a person identifiable by the "prankster", which

determines that the data of the voice of said identifiable person must be considered data

staff.

The data protection regulations, therefore, do not restrict the concept of "personal data".

personal" or "identifiable person" exclusively in the event that the person responsible for the

treatment is who can identify, directly or indirectly, the interested party whose data

are treated (the overwhelmed), but extends its perimeter of protection beyond said

circumstance and considers that if said person (the overwhelmed), as a consequence of the

means made available to the prankster by the person in charge (MIRACLIA), -such as the

singularization (by the voice, for example)-, can be identified, directly or indirectly,

by "any other person" other than the person responsible, (and this even though said overwhelmed person is not

identifiable for the person in charge, since it is not required to be so) considers said

information as personal data referring to a natural person, and therefore it is applicable

data protection regulations.

In the event that it is considered that there are two joint controllers with respect to

of the same treatment, the CJEU has taken care to emphasize that the protection regulations

of data does not require or imply that each of them has access to personal data in

matter, so there may be some of those responsible who, without having access to the

personal data will continue to be responsible (see section 69 of the judgment of 29

July 2019, C-40/17, Fashion ID, which in turn cites section 29 of the judgment of 5

June 2018, C-210/16, Wirtschaftakademie Schleswig-Holstein, and paragraph 65 of the

Judgment of July 10, 2018, C-25/17, Jehovah's Witnesses).

Article 5 “Principles related to treatment” of the RGPD establishes:

“1. The personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party ("lawfulness, loyalty and transparency");

b) collected for specific, explicit and legitimate purposes, and will not be further processed in manner incompatible with those purposes; according to article 89, paragraph 1, the treatment further processing of personal data for archiving purposes in the public interest, research purposes scientific and historical or statistical purposes shall not be considered incompatible with the initial purposes (“purpose limitation”);

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which they are processed (“data minimization”);

d) accurate and, if necessary, updated; All reasonable steps will be taken to Personal data that is inaccurate with respect to the data is deleted or rectified without delay. purposes for which they are processed (“accuracy”);

e) kept in a way that allows the identification of the interested parties for no more than the necessary for the purposes of the processing of personal data; personal data may be kept for longer periods as long as they are treated exclusively for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1), without prejudice to the application of technical and organizational measures appropriate measures imposed by this Regulation in order to protect the rights and freedoms of the interested party (“limitation of the retention period”);

f) processed in such a way as to ensure adequate security of the personal data, including protection against unauthorized or unlawful processing and against loss, destruction or damage accident, through the application of appropriate technical or organizational measures ("integrity and confidentiality").

2. The controller will be responsible for compliance with the provisions of section 1

and able to demonstrate it (“proactive responsibility”)”.

In relation to the aforementioned principles, what is stated in the

Considering 39 of the aforementioned RGPD:

“39. All processing of personal data must be lawful and fair. For individuals, you must

be absolutely clear that they are being collected, used, accessed or otherwise processed

personal data that concerns them, as well as the extent to which said data is or will be processed.

The principle of transparency requires that all information and communication regarding the processing of

said data is easily accessible and easy to understand, and that simple and clear language is used.

This principle refers in particular to the information of the interested parties on the identity of the

responsible for the treatment and the purposes of the treatment and to the information added to guarantee a

fair and transparent treatment with respect to the affected natural persons and their right to

obtain confirmation and communication of the personal data that concern them that are the object of

treatment. Natural persons must be aware of the risks, standards,

safeguards and the rights related to the processing of personal data as well as the way of

assert their rights in relation to the treatment. In particular, the specific purposes of the

processing of personal data must be explicit and legitimate, and must be determined in the

time of collection. Personal data must be adequate, relevant and limited to what is

necessary for the purposes for which they are processed. This requires, in particular, ensuring that

Limit your retention period to a strict minimum. Personal data should only be processed if the

purpose of the treatment could not reasonably be achieved by other means. To ensure that

personal data is not kept longer than necessary, the data controller must

establish deadlines for its deletion or periodic review. All measures must be taken

reasonable steps to ensure that inaccurate personal data is rectified or deleted.

Personal data must be processed in a way that guarantees security and confidentiality

of personal data, including to prevent unauthorized access or use of said data.

data and the equipment used in the treatment.



7th

Article 4 of the RGPD, under the heading "Definitions", provides the following:

“2) «treatment»: any operation or set of operations carried out on personal data or sets of personal data, whether by automated procedures or not, such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, broadcast or any other form of authorization of access, collation or interconnection, limitation, suppression or destruction”.

In accordance with these definitions, the use that said entity makes of the information (personal data) that it collects from the harassed person constitutes a processing of personal data, in respect of which the controller must comply with the principles established in article 5.1 of the RGPD, according to which personal data will be "treated in a lawful, loyal and transparent manner in relation to the interested party (legality, loyalty and transparency)”; and developed in Chapter III, Section 1, of the same Regulation (articles 12 and following).

Article 12.1 of the aforementioned Regulation establishes the obligation of the person responsible for treatment to take the appropriate measures to “provide the interested party with all information indicated in articles 13 and 14, as well as any communication in accordance with the articles 15 to 22 and 34 regarding the treatment, in a concise, transparent, intelligible and easily accessible, with clear and simple language, in particular any information addressed to child. The information will be provided in writing or by other means, including, if applicable,

by electronic means. When requested by the interested party, the information may be provided verbally provided that the identity of the interested party is proven by other means.

Article 13 of the aforementioned legal text details the “information that must be provided when the personal data is obtained from the interested party” and article 14 of the same Regulation refers to the “information that must be provided when the personal data have not been obtained from the interested party”.

In the first case, when the personal data is collected directly from the interested party, the information must be provided at the very moment in which that data Collect. Article 13 of the RGPD details this information in the terms following:

"1. When personal data relating to him is obtained from an interested party, the person in charge of the treatment, at the time these are obtained, will provide all the information indicated to continuation:

a) the identity and contact details of the person in charge and, where appropriate, of his representative;

b) the contact details of the data protection delegate, if any;

c) the purposes of the treatment to which the personal data is destined and the legal basis of the treatment;

d) when the treatment is based on article 6, paragraph 1, letter f), the legitimate interests of the responsible or a third party;

e) the recipients or categories of recipients of the personal data, if applicable;

f) where appropriate, the intention of the controller to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or, in the case of transfers indicated in articles 46 or 47 or article 49, paragraph 1, second paragraph, reference to the adequate or appropriate guarantees and the means to obtain a

copy of these or the fact that they have been lent.

2. In addition to the information mentioned in section 1, the data controller shall provide the interested, at the time the personal data is obtained, the following information necessary to guarantee fair and transparent data processing:

a) the period during which the personal data will be kept or, when this is not possible, the criteria used to determine this term;

b) the existence of the right to request access to personal data from the data controller related to the interested party, and its rectification or deletion, or the limitation of its treatment, or to oppose the treatment, as well as the right to data portability;

c) when the treatment is based on article 6, paragraph 1, letter a), or article 9, paragraph 2, letter a), the existence of the right to withdraw consent at any time, without affecting to the legality of the treatment based on the consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or a necessary requirement to sign a contract, and if the interested party is obliged to provide personal data and is informed of the possible consequences of not providing such data;

f) the existence of automated decisions, including profiling, referred to in article 22, paragraphs 1 and 4, and, at least in such cases, significant information on the logic applied, as well as the importance and the anticipated consequences of said treatment for the interested.

3. When the data controller plans the further processing of personal data for a purpose other than that for which they were collected, will provide the interested party, prior to said further processing, information about that other purpose and any additional information relevant to the of section 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and to the extent that the

interested party already has the information".

In the second case, when the personal data is not obtained from the interested party, the

information that must be provided to it is established in article 14 of the RGPD:

"1. When the personal data has not been obtained from the interested party, the data controller

will provide you with the following information:

a) the identity and contact details of the person in charge and, where appropriate, of his representative;

b) the contact details of the data protection delegate, if any;

c) the purposes of the processing for which the personal data is intended, as well as the legal basis for the processing.

treatment;

d) the categories of personal data in question;

e) the recipients or categories of recipients of the personal data, if any;

f) Where appropriate, the intention of the controller to transfer personal data to a recipient in a

third country or international organization and the existence or absence of an adequacy decision

the Commission, or, in the case of transfers indicated in articles 46 or 47 or article 49,

section 1, second paragraph, reference to the adequate or appropriate guarantees and the means to

obtain a copy of them or the fact that they have been loaned.

2. In addition to the information mentioned in section 1, the data controller shall provide the

interested party the following information necessary to guarantee a fair treatment of data and

transparent with respect to the interested party:

a) the period during which the personal data will be kept or, when this is not possible, the

criteria used to determine this term;

b) when the treatment is based on article 6, paragraph 1, letter f), the legitimate interests of the

data controller or a third party;

c) the existence of the right to request access to personal data from the data controller

related to the interested party, and its rectification or deletion, or the limitation of its treatment, and to oppose the treatment, as well as the right to data portability;

d) when the treatment is based on article 6, paragraph 1, letter a), or article 9, paragraph 2, letter a), the existence of the right to withdraw consent at any time, without affecting to the legality of the treatment based on the consent before its withdrawal;

e) the right to file a claim with a supervisory authority;

f) the source from which the personal data comes and, where appropriate, if they come from access sources public;

g) the existence of automated decisions, including profiling, referred to in article 22, paragraphs 1 and 4, and, at least in such cases, significant information on the logic applied, as well as the importance and the anticipated consequences of said treatment for the interested.

3. The controller will provide the information indicated in sections 1 and 2:

a) within a reasonable period of time, once the personal data has been obtained, and at the latest within a month, taking into account the specific circumstances in which said data is processed;

b) if the personal data is to be used for communication with the interested party, no later than the time of the first communication to said interested party, or

c) if it is planned to communicate them to another recipient, at the latest at the time the data personal data are communicated for the first time.

4. When the person in charge of the treatment projects the subsequent treatment of the personal data for a purpose other than that for which they were obtained, will provide the interested party, before said further processing, information about that other purpose and any other relevant information indicated in

section 2.

5. The provisions of sections 1 to 4 shall not apply when and to the extent that:

a) the interested party already has the information;

b) the communication of said information is impossible or supposes a disproportionate effort,

in particular for processing for archiving purposes in the public interest, research purposes

scientific or historical or statistical purposes, subject to the conditions and guarantees indicated in the

Article 89, paragraph 1, or insofar as the obligation mentioned in paragraph 1 of the

This article may make it impossible or seriously impede the achievement of the objectives of such

treatment. In such cases, the person in charge will adopt adequate measures to protect the rights,

liberties and legitimate interests of the interested party, including making the information public;

c) the obtaining or communication is expressly established by the Law of the Union or of the

Member States that applies to the data controller and establishes measures

adequate to protect the legitimate interests of the interested party, or

d) when the personal data must remain confidential on the basis of a

obligation of professional secrecy regulated by the Law of the Union or of the Member States,

including an obligation of secrecy of a statutory nature".

For its part, article 11.1 and 2 of the LOPDGDD provides the following:

"Article 11. Transparency and information to the affected

1. When the personal data is obtained from the affected party, the data controller may give

compliance with the duty of information established in article 13 of Regulation (EU) 2016/679

providing the affected party with the basic information referred to in the following section and indicating

an electronic address or other means that allows easy and immediate access to the

remaining information.

2. The basic information referred to in the previous section must contain, at least:

a) The identity of the data controller and his representative, if any.

b) The purpose of the treatment.

c) The possibility of exercising the rights established in articles 15 to 22 of the Regulation (EU)



2016/679.

If the data obtained from the affected party were to be processed for profiling, the basic information will also include this circumstance. In this case, the affected party must be informed of their right to oppose the adoption of automated individual decisions that produce legal effects on him or significantly affect him in a similar way, when he attends this right in accordance with the provisions of article 22 of Regulation (EU) 2016/679".

In relation to this principle of transparency, it is also taken into account expressed in Recitals 32, 39 (already outlined), 42, 47, 58, 60 and 61 of the RGPD. I know reproduces below part of the content of these Considerations:

(32) Consent must be given through a clear affirmative act that reflects a manifestation of free, specific, informed, and unequivocal will of the interested party to accept data processing of a personal nature that concern you…

(42) …For the consent to be informed, the interested party must know at least the identity of the data controller and the purposes of the processing for which the data is intended. personal information…

(47) The legitimate interest of a data controller, including that of a data controller may communicate personal data, or of a third party, may constitute a legal basis for the treatment, provided that the interests or the rights and freedoms of the interested party do not prevail, taking into account the reasonable expectations of the interested parties based on their relationship with the responsible… In any case, the existence of a legitimate interest would require an evaluation

meticulous, even if a data subject can reasonably foresee, at the time and in the

context of the collection of personal data, which may be processed for this purpose. In

In particular, the interests and fundamental rights of the interested party may prevail over the

interests of the data controller when processing personal data

in circumstances in which the interested party does not reasonably expect that a treatment will be carried out

subsequent…

(58) The principle of transparency requires that all information addressed to the public or the interested party be

concise, easily accessible and easy to understand, and that clear and simple language is used, and,

In addition, in your case, it is displayed...

(60) The principles of fair and transparent processing require that the data subject be informed of the

existence of the processing operation and its purposes. The data controller must provide the

interested as much additional information as necessary to guarantee a fair treatment and

transparent, taking into account the specific circumstances and context in which the

personal information. The interested party must also be informed of the existence of the preparation of

profiles and the consequences of said elaboration. If personal data is obtained from

interested parties, they must also be informed of whether they are obliged to provide them and of the consequences

in case they didn't...

(61) Data subjects should be provided with information on the processing of their personal data in

the time they are obtained from them or, if obtained from another source, within a reasonable time,

depending on the circumstances of the case...

The Constitutional Court, among others, in its STC 39/2016, of March 3, with appointment

in turn of the STC 292/2000, of November 30, has established that the right of

information is part of the essential content of the right to data protection. Thus, in

its FJ2, from STC 39/2016, states:

“The duty of prior information is part of the essential content of the right to protection of

data, as it is an essential complement to the need for consent of the affected party.

The duty of information on the use and destination of personal data required by the Organic Law of protection of personal data is closely linked to the general principle of consent for the processing of data, because if its purpose and recipients are not known, consent can hardly be given. Therefore, when assessing whether the right to data protection for breach of the duty of information, the waiver of Consent to data processing in certain cases must be an element to take into account. given the close link between the duty of information and the general principle of consent.

(…)

Thus, they are characteristic elements of the constitutional definition of the fundamental right to protection of personal data «the rights of the affected party to consent to the collection and use of their personal data and to know about them. And they are essential to make this content the recognition of the right to be informed of who owns your personal data and with what purpose, and the right to be able to oppose that possession and use, requiring whoever it corresponds to terminate the possession and use of the data. In other words, requiring the owner of the file to inform of what data you have about your person, accessing your appropriate records and seats, and what destination have had, which also reaches potential assignees; and, where appropriate, require you to rectify or cancel them" (STC 292/2000, of November 30, FJ 7)".

MIRACLIA does not inform the interested party at any time, that is, the overwhelmed person, of the content of your rights in accordance with the provisions of the RGPD. This determines that the The processing of data that it carries out in no case can be considered lawful.

Article 12.1 of the RGPD establishes that said information must be provided "by

written"; Only if requested by the interested party, the information may be provided verbally, always

that the identity of the interested party be proven by other means. In the present case, there has been no

there has been no information in writing, nor has the identity of the interested party been

proven by any means.

Article 13.1 of the RGPD establishes that “when they are obtained from an interested party

personal data relating to him” (as is the case, since the call is made to the

overwhelmed and therefore the personal data, your voice, comes directly from the overwhelmed),

the person in charge of the treatment, "at the moment in which these [the data] are obtained",

will provide all the information indicated below in that section.

As can be seen from the facts of the file, MIRACLIA has not informed

previously of any of said circumstances to the overwhelmed, so that the

fundamental right to data protection of the overwhelmed, who have not had

knowledge, prior to the recording that MIRACLIA always performs of your data in

their systems, of the circumstances that the regulations establish that they must know.

The affected person answers a phone call, which will be recorded, not only without

having been able to give their consent, but without having been informed, at that time, of

so that you are aware of the treatment that is intended to be carried out with your data

and the circumstances required by the regulations for the protection of the right

fundamental. Among these circumstances, it is worth highlighting the one provided for in letter c) of section

1 of said article 13 of the RGPD: the interested party must be informed at the time of

obtaining your personal data, among other circumstances, from the legal basis of the

treatment, to which it is possible to add what is established in letter d), that is, that when the

treatment is based on art. 6, section 1, letter f) -legitimate interest-, the

interested party what are the legitimate interests of the person in charge or of a third party that are alleged

as a legal basis for processing.

This lack of information on what is the legal basis of the treatment or in case of claim legitimate interest, what are those legitimate interests, is of great importance. The RGPD intends that the interested party (the overwhelmed) may have knowledge at that time (at the time of collecting your personal data) what are the legitimate interests that are hypothetically alleged by the controller to process your personal data without need for your consent. It is at this moment when it will have to be done by the responsible for the treatment the weighting between the legitimate interests that could be claim by the person in charge and the interests or fundamental rights and freedoms of the interested party that require the protection of their personal data, in particular when the interested is a child. Such weighting cannot be done at a later time, unilaterally by the controller, without taking into account the rights, freedoms and interests of the overwhelmed himself, for it is simply enough to say that he would be denied not only his right to information, but their right to make allegations, to be heard before the claim of the responsible for using your personal data without your consent (because that is precisely the virtuality of the use of legitimate interest as a legal basis for treatment, and what MIRACLIA intends here as data controller).

The CJEU ruling of July 29, 2019, C-40/17, Fashion ID, establishes the guidelines of who would correspond, in any case, to request the consent of the interested in the event that there are two, or more, data controllers. As well as It also determines who is responsible for the information obligation to the interested party, and When should this information be given? And from this sentence it turns out that, applying it to the

present case, it would correspond to MIRACLIA.

Sections 102 to 104 of the Fashion ID ruling establish:

“102 With regard to the consent mentioned in articles 2, letter h), and 7, letter a), of Directive 95/46, it turns out that this must occur prior to collection and communication by transmission of data of the interested party. In these circumstances, it is up to the site administrator to Internet, and not the provider of the social module, request such consent, to the extent that it is the fact that a visitor consults that Internet site which triggers the process of treatment of personal data. Indeed, as the Advocate General pointed out in point 132 of his conclusions, it would not be consistent with an effective and timely protection of the rights of the interested party that the consent was only given to the co-responsible for the treatment that intervenes subsequently, namely to the supplier of said module. However, the consent that must be lend to the administrator refers only to the operation or to all the operations of processing of personal data whose purposes and means are effectively determined by said administrator.

103 The same can be said with respect to the information obligation established in article 10 of Directive 95/46.

104 From the wording of that provision it is clear, in this regard, that the person responsible for the treatment or its representative must inform the person from whom the data is collected by what minus the information mentioned in the aforementioned provision. Therefore, it turns out that the person responsible of the treatment must give said information immediately, that is, at the moment in which it is collect the data (see, in this sense, the judgments of May 7, 2009, Rijkeboer, C-553/07, EU:C:2009:293, section 68, and of November 7, 2013, IPI, C-473/12, EU:C:2013:715, paragraph 23)”.

As is known, there is no unlimited right and the right to information of the interested, as an essential part of the fundamental right to the protection of your data personal, is not alien to this principle. Now then, as an exception it will have to be

interpreted strictly, so that only in the cases established by

the law may be understood that there may be an exception to the right to information.

As established in section 39 of the STJUE of November 7, 2013, C-

473/12, Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and others,

which we will refer to later:

39 According to settled jurisprudence, the protection of the fundamental right to privacy requires

that the exceptions to the protection of personal data and the restrictions to such protection are

established without exceeding the limits of what is strictly necessary (decisions of December 16

2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, Rec. p. I-9831, section 56, and of 9 of

November 2010, Volker and Markus Schecke and Eifert, C-92/09 and C-93/09, Rec. p. I-11063,

paragraphs 77 and 86).

The only limitations to the right to information are found in article 23 of the

RGPD and express legislative measures are needed to agree on them, respecting in all

case the essential rights and freedoms, and provided that the assumptions assessed

that are listed in the provision.

Although in reference to consent, MIRACLIA has indicated that it cannot

address some regulatory provisions because the very fact of spending

a joke or the surprise effect. However, nothing has been alleged regarding the limitations

indicated, nor do they appear to be applicable to the present case. MIRACLIA not

does not mention any legislative measure that entails the possibility of exceptions in the case

of the application ***APPLICATION.1 the fundamental right to data protection

personal information of the interested party, the overwhelmed one, so that any subsequent analysis would lack

sense. In addition, the possibility of exempting through legislative measures the rights fundamental rights of individuals are of such importance as the security of the state, the defense, public safety, the prevention, investigation, detection or prosecution of criminal offenses etc. So that in no case said possibility of excluding the right of information of the interested party is tied to the possibility of playing jokes through of an online application, nor to a commercial interest, so there can be no commercial interests that serve as justification for the concerned-absorbed to be deny your right to be informed in the terms of article 13 RGPD.

Therefore, the performance of MIRACLIA is not excluded from the obligation to provide interested parties with the right to information, with the content established in the article 13 RGPD, at the time the personal data is obtained from the interested party.

When the personal data is obtained from the interested party, in no case said information can be provided later, let alone never be given, as is the case here occupies us. In short, the interested parties must in any case be informed so that the treatment can be considered lawful, which has certainly not been the case.

The same can be said about compliance with the provisions of article 14 of the RGPD, which regulates the information that must be offered to the interested party when the data is not are collected directly from it, as occurs in relation to the telephone number mobile of the overwhelmed, which is provided to MIRACLIA by a third party, the joker.

In general, no information is offered by MIRACLIA to the interested/affected person (person who receives the prank call) in the documents “Terms and Conditions of Use of the Service” and “Privacy Policy”, beyond indicating that “Miraclia does not collect data from the

recipients of the jokes", which, as has been seen, is not true.

The only information addressed to the overwhelmed person results from the locution that is reproduced end of the prank call, with the following message:

"A friend of yours has played a prank on you. In case you don't want your friend to be able to listen to, download or spread the joke, or in case you do not want to receive any more jokes, press 5 with your keyboard after the signal. Beep".

As can be seen, in said locution it is not specified that the joke was recorded and that, through the indicated action, be erased from the entity's systems. Nope otherwise, details about none of the aspects established in the articles 13 and 14 of the RGPD.

On the other hand, at no time during the telephone conversation did identifies the application ***APPLICATION.1 as manager of the call or the company developer MIRACLIA as the owner of the platform, so that the recipient of the prank does not know where to go for more information about the call or exercise your rights; at no time is the joker quoted; and I don't know either informs at no time, during the development of the joke, that the conversation is being or may be recorded.

Consequently, the exposed facts suppose a violation of the principle of transparency regulated in articles 13 and 14 of the RGPD, which gives rise to the application of the corrective powers that article 58 of the aforementioned Regulation grants to the Agency Spanish Data Protection.

Finally, it should be noted that MIRACLIA has argued that, due to the present proceedings, knowing the accusation made for the first time in relation to the information defects, has immediately proceeded to correct them by completing the information offered at the end of the prank conversation as follows:

- That someone has played a joke to have a good time for both of them.

- That for the same has used the application ***APPLICATION.1 property of

MIRACLIA TELECOMMUNICATIONS, S.L.

- That to oppose said prank reaching the prankster and to suppress it can

press key 5.

- Who has more information by pressing the 1 key.

And pressing key 1 offers a detailed explanation, also included on the web.

In this way, from the information that was not provided to the interested party, it has now included:

- The identity of MIRACLIA

- The contact details of the Data Protection Officer

- The term of conservation

- The basis of legitimation

- The exercise of the rights in full, although those of opposition and

delete (and also access when requested) are now specified

formally.

He does not, however, provide any proof of this; not even the text or recording

of the phrase inserted at the end of the conversation, so that it can be assessed



correctly the supposed information offered. And neither does MIRICLIA point out anything about

of the precautions adopted to ensure that the interested party has effectively agreed

to the information or on the measures that it will apply in those cases in which it is interrupted

communication before the reproduction of the locution.

viii

On the other hand, articles 6 and 7 of the same RGPD refer, respectively, to the

“Legality of treatment” and the “Conditions for consent”:

Article 6 of the RGPD.

"1. The treatment will only be lawful if at least one of the following conditions is met:

a) the interested party gave his consent for the processing of his personal data for one or more

specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is a party or for

the application at the request of the latter of pre-contractual measures;

c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person in charge

of the treatment;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the

exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the

responsible for the treatment or by a third party, provided that said interests do not prevail

interests or the fundamental rights and freedoms of the interested party that require the protection of

personal data, in particular when the data subject is a child.

The provisions of letter f) of the first paragraph shall not apply to the treatment carried out by the

public authorities in the exercise of their functions.

2. Member States may maintain or introduce more specific provisions in order to

adapt the application of the rules of this Regulation with regard to the treatment in

compliance with section 1, letters c) and e), establishing more precisely specific requirements of

processing and other measures to ensure fair and lawful processing, including other

specific treatment situations under chapter IX.

3. The basis of the treatment indicated in section 1, letters c) and e), must be established by:

a) Union law, or

b) the law of the Member States that applies to the data controller.

The purpose of the treatment must be determined in said legal basis or, in relation to the

treatment referred to in section 1, letter e), will be necessary for the fulfillment of a mission

carried out in the public interest or in the exercise of public powers conferred on the person responsible for the

treatment. This legal basis may contain specific provisions to adapt the application

of rules of this Regulation, among others: the general conditions that govern the legality of the

treatment by the controller; the types of data object of treatment; the interested

affected; the entities to which personal data can be communicated and the purposes of such

communication; purpose limitation; the terms of conservation of the data, as well as the

processing operations and procedures, including measures to ensure a

lawful and equitable treatment, such as those related to other specific situations of treatment under

of chapter IX. The Law of the Union or of the Member States will fulfill an objective of interest

public and will be proportional to the legitimate aim pursued.

4. When processing for a purpose other than that for which the personal data was collected

is not based on the consent of the interested party or on the Law of the Union or of the States

members that constitutes a necessary and proportionate measure in a democratic society to

safeguard the objectives indicated in article 23, paragraph 1, the controller, with



in order to determine if the treatment for another purpose is compatible with the purpose for which they were collected

initially the personal data, will take into account, among other things:

a) any relationship between the purposes for which the personal data were collected and the purposes

of the envisaged further treatment;

b) the context in which the personal data were collected, in particular as regards the

relationship between the interested parties and the data controller;

c) the nature of the personal data, specifically when special categories of data are processed

personal, in accordance with article 9, or personal data relating to convictions and offenses

criminal, in accordance with article 10;

d) the possible consequences for data subjects of the envisaged further processing;

e) the existence of adequate guarantees, which may include encryption or pseudonymization".

Article 7 of the RGPD.

"1. When the treatment is based on the consent of the interested party, the person in charge must be

able to demonstrate that he consented to the processing of his personal data.

2. If the data subject's consent is given in the context of a written statement that is also

refers to other matters, the request for consent will be presented in such a way that it is distinguished

clearly from other matters, in an intelligible and easily accessible manner and using clear language

And simple. Any part of the declaration that constitutes an infringement of this document will not be binding.

Regulation.

3. The interested party shall 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 its

withdrawal. Before giving their consent, the interested party will be informed of it. It will be so easy to remove the

consent how to give it.

4. In assessing whether consent has been freely given, account shall be taken to the greatest extent

possible whether, among other things, the performance of a contract, including the provision of a

service, is subject to consent to the processing of personal data that is not necessary

for the performance of said contract.

It takes into account what is expressed in recitals 32, 39, 40 to 44 and 47 of the RGPD

in relation to the provisions of articles 6 and 7 above.

It is also appropriate to take into account the provisions of article 6 of the LOPDGDD:

“Article 6. Treatment based on the consent of the affected party

1. In accordance with the provisions of article 4.11 of Regulation (EU) 2016/679, it is understood

By consent of the affected party, any manifestation of free will, specific, informed and

unequivocal by which he accepts, either by means of a declaration or a clear affirmative action, the

processing of personal data concerning you.

2. When it is intended to base the processing of the data on the consent of the affected party for a

plurality of purposes, it will be necessary to state specifically and unequivocally that said

Consent is granted for all of them.

3. The execution of the contract may not be subject to the affected party consenting to the treatment of the data.

personal data for purposes that are not related to the maintenance, development or control

of the contractual relationship.

In accordance with what has been expressed, data processing requires the existence of a

legal basis that legitimizes it, such as the consent of the interested party validly provided,

necessary when there is no other legal basis mentioned in article 6.1

of the RGPD or the treatment pursues a purpose compatible with that for which the data were collected.

data.



Article 4 of the GDPR defines "consent" in the following terms:

“Article 4 Definitions

For the purposes of this Regulation, the following shall be understood as:

11. «consent of the interested party»: any expression of free, specific, informed and

unequivocal by which the interested party accepts, either through a declaration or a clear action affirmative, the treatment of personal data that concerns you".

Consent is understood as a clear affirmative act that reflects a free, specific, informed and unequivocal manifestation of the interested party's accept the treatment of personal data that concerns you, provided with sufficient guarantees to prove that the interested party is aware of the fact that he gives his consent and the extent to which it does so. And it must be given for all the activities of treatment carried out with the same or the same purposes, so that, when the treatment has several purposes, consent must be given for all of them in a specific and unequivocal, without the execution of the contract being subject to the consent of the affected party. the processing of your personal data for purposes that are not related to the maintenance, development or control of the business relationship. In this regard, the legality of the Treatment requires that the interested party be informed about the purposes for which the data is intended. data (informed consent).

Consent must be given freely. It is understood that consent is free when the interested party does not enjoy a true or free choice or cannot refuse or withdraw your consent without prejudice; or when you are not allowed to authorize by separate the different personal data processing operations despite being adequate in the specific case, or when the fulfillment of a contract or provision of service is dependent on consent, even when consent is not necessary for said consent. compliance. This occurs when consent is included as a non-part negotiable of the general conditions or when the obligation to be in compliance is imposed. agreement with the use of personal data in addition to those strictly necessary.

Without these conditions, the provision of consent would not offer the data subject a true control over your personal data and its destination, and this would make it illegal treatment activity.

The Article 29 Working Group analyzed these issues in its document

“Guidelines on consent under Regulation 2016/679”, revised and

approved on 04/10/2018; which has been updated by the European Committee for the Protection of

Data on 05/04/2020 through the document “Guidelines 05/2020 on consent

in accordance with Regulation 2016/679”. From what is indicated in this document, it is now interesting

highlight some aspects related to the validity of consent, specifically

on the elements “specific”, “reported” and “unequivocal”:

<<3.2. Specific declaration of will

Article 6, paragraph 1, letter a), confirms that the consent of the interested party for the treatment of

your data must be given "for one or more specific purposes" and that an interested party can choose with

for each of these purposes. The requirement that consent must be “specific”

Its purpose is to guarantee a level of control and transparency for the interested party. This requirement has not

been modified by the GDPR and remains closely linked to the requirement of

informed consent". At the same time, it must be interpreted in line with the requirement of

"dissociation" to obtain "free" consent. In short, to fulfill the character of



“specific” the data controller must apply:

i) specification of the purpose as a guarantee against deviation from use,

ii) dissociation in consent requests, and

iii) a clear separation between the information related to obtaining consent for the

data processing activities and information relating to other matters.

Ad. i): In accordance with article 5, paragraph 1, letter b), of the RGPD, obtaining the

Valid consent is always preceded by the determination of a specific, explicit and

legitimate for the intended treatment activity. The need for specific consent in

combination with the notion of purpose limitation in Article 5(1)(b),

works as a guarantee against the gradual expansion or blurring of the purposes for which it is

performs the processing of the data once an interested party has given their authorization for the collection

initial data. This phenomenon, also known as diversion of use, poses a risk

for the interested parties since it may lead to an unforeseen use of personal data by the user.

responsible for the treatment or third parties and the loss of control by the interested party.

If the data controller relies on Article 6(1)(a), the data subjects

They must always give their consent for a specific purpose for data processing. In

in line with the concept of purpose limitation, with article 5, paragraph 1, letter b), and with

recital 32, the consent may cover different operations, provided that said

operations have the same purpose. Needless to say, specific consent can only

obtained when the interested parties are expressly informed about the intended purposes for the use of

the data that concerns them.

Without prejudice to the provisions on the compatibility of purposes, the consent must be

specific for each purpose. The interested parties will give their consent on the understanding that they have control

about your data and that these will only be treated for those specific purposes. If a person in charge treats

data based on consent and, in addition, you want to process said data for another purpose, you must

obtain consent for that other purpose, unless there is another legal basis that better reflects the

situation…

Ad. ii) Consent mechanisms should not only be separated in order to fulfill the

requirement of "free" consent, but must also comply with the consent

"specific". This means that a data controller seeking consent to

several different purposes, you must facilitate the possibility of opting for each purpose, so that users

may give specific consent for specific purposes.

Ad. iii) Finally, data controllers must provide, with each data request,

separate consent, specific information on the data that will be processed for each purpose, with the

in order that the interested parties know the repercussion of the different options that they have. of this

In this way, data subjects are allowed to give specific consent. This issue overlaps with the

requirement that controllers provide clear information, as set out above

in section 3.3>>.

<<3.3. Manifestation of informed will

The GDPR reinforces the requirement that consent must be informed. In accordance with the

article 5 of the RGPD, the requirement of transparency is one of the fundamental principles,

closely related to the principles of loyalty and legality. Provide information to

data subjects before obtaining their consent is essential for them to be able to make decisions

informed, understand what they are authorizing and, for example, exercise their right to withdraw

Your consent. If the person in charge does not provide accessible information, the control of the user will be

illusory and consent will not constitute a valid basis for data processing.

If the requirements regarding informed consent are not met, the consent will not be

valid and the person in charge may be in breach of article 6 of the RGPD.

3.3.1. Minimum content requirements for consent to be “informed”

In order for the consent to be informed, it is necessary to communicate to the interested party certain elements

that are crucial to be able to choose. Therefore, the WG29 believes that it is required, at least, the



following information to obtain valid consent:

i) the identity of the data controller,

ii) the purpose of each of the treatment operations for which consent is requested,

iii) what (type of) data will be collected and used,

iv) the existence of the right to withdraw consent,

v) information on the use of data for automated decisions in accordance with the

article 22, paragraph 2, letter c), when relevant, and

vi) information on the possible risks of data transfer due to the absence of a

decision of adequacy and adequate guarantees, as described in article 46>>.

In the present case, MIRACLIA affirms in its arguments that consent does not

can be the legal basis for playing a joke, thereby understanding that the treatment

of the personal data of the abromados that it carries out is protected by the legitimate interest of the

article 6.1.f) of the RGPD.

However, that is not what emerges from the information inserted in the

document called "Terms and Conditions of Use of the Service" (Proven Fact

Second), in which it is indicated up to three times that the user must have the

express and unequivocal consent of the person who has received the joke so that

the recording can be made and the audio file can be shared later, as a requirement

of operation of the service ("The operation of the Service prevents the generation of

a Recording if the user of ***APPLICATION.1 does not expressly accept such condition

previous"). In said document, MIRACLIA expressly declares that "it is not responsible

of the consequences of failure to obtain the necessary consents

to share the Recording".

In other words, MIRACLIA bases the processing of personal data directly on the

consent of the "overwhelmed", which must be obtained by the "prankster" himself.

MIRACLIA is aware, then, that said legal basis for processing is

merely formal, fictitious. If you consider that a joke can never be based on the

consent of the abominated himself, what is indicated in his outlined document is not understood,

knowing that the prankster will never proceed to seek the consent of the overwhelmed.

On the other hand, the processing of personal data carried out by the data controller

MIRACLIA treatment in no case can be considered "lawful" since it is not

provides the interested party with the information to which, in accordance with the data protection regulations,

personal data, you have the right, as concluded in the Legal Basis

previous.

Nor can it be considered lawful from the moment in which, as there is no such

information, the interested party is deprived of his right to know the legal basis of the

treatment alleged by the person in charge, and specifically, when referring to the legitimate interest, it is seen

deprived of his right to know what are said legitimate interests alleged by the

responsible or of a third party that would justify the treatment without taking into account its

consent.

In the same way, the interested party is deprived of his right to claim for what reasons

Said legitimate interest alleged by the person in charge could be counteracted by the rights

or interests of the interested party. Not having given the interested party the opportunity to claim them

vis-à-vis the person in charge, any assessment made by the person in charge without taking into account



the circumstances that could be alleged by the interested party who has not been allowed to do so

would be vitiated, for being an act contrary to an imperative norm.

If the rule requires that the subject be informed of their rights, and this is not done, the

consequence must be the nullity of subsequent acts (the same weighting made

would be null and void, as well as the same data processing

made on a null weighting and without any value).

On the other hand, there is no legal measure that exempts said obligation to

provide the aforementioned information by the person in charge, as stated.

Therefore, it cannot be understood that it is applicable as a legal basis for the treatment

of personal data that of the legitimate interest provided for in article 6.1.f) of the RGPD.

However, although we understand that the legitimate interest is not applicable, it is of interest

hypothetically analyze the terms in which the weighing that foresees should be carried out

said article between the legitimate interest of the data controller and data protection

of a personal nature of the interested party, that is, how said legitimate interest plays, if it were

applicable.

Well, if this were the case, the CJEU, already in its ruling of May 4, 2017,

C-13/16, Rigas Satskime, paragraph 28 to 34, determined what are the requirements for a

processing may be lawful on the basis of legitimate interest. The CJEU ruling of 29

July 2019, C-40/17, Fashion ID, echoing the aforementioned ruling, collects said

requirements.

28 In this regard, article 7, letter f), of Directive 95/46 -(current article 6.1.f) of the RGPD)- establishes

three cumulative requirements for the processing of personal data to be lawful: first, that the

responsible for the treatment or the third party or third parties to whom the data is communicated pursue a

legitimate interest; second, that the treatment is necessary for the satisfaction of that interest

legitimate and, third, that the fundamental rights and freedoms of the interested party do not prevail in the

data protection.

Regarding the first of the requirements, that is, that the data controller or

third parties pursue a legitimate interest, we are faced with a commercial interest, which could

be considered legitimate in itself, focused on making money by selling jokes

To thirds. However, these benefits are obtained at the cost of affecting the rights and

legitimate interests to the protection of your personal data of the interested parties (overwhelmed),

Therefore, said interest must be weighed against that of individuals.

For what the second of the requirements does, however, we consider that the processing of personal data that is carried out by the appellant is not necessary or strictly necessary for the satisfaction of its legitimate interest (the cited judgment of 4 May 2017, C-13/16, Rigas Satskime, in its section 30, declares “As regards the requirement that data processing is necessary, it should be remembered that the exceptions and restrictions to the principle of protection of personal data must be established without exceeding the limits of what is strictly necessary”).

This principle that processing must be strictly necessary for the satisfaction of legitimate interest must be interpreted in accordance with the provisions of article 5.1.c) RGPD, which refers to the principle of data minimization,



stating that the personal data will be “adequate, pertinent and limited to what is necessary in relation to the purposes for which they are processed”.

Leaving aside, as we have already mentioned, the issue that the concerned/approached does not know for what purposes or on what legal basis their data has been collected data, it is understood that the recording of the voice of the interested parties in the MIRACLIA, which is carried out in all cases and in all circumstances, as well as equally, as It has been revealed in the administrative file, that the telephone numbers of the interested parties are saved in said systems until the call is made, it supposes a excessive treatment. If the legitimate interest pursued is to collect so that a person, the joker, can play a joke, it does not seem necessary, as an intrinsic requirement of said

treatment, (i) the storage of personal data (telephone and voice). can't either

considered legitimate, and therefore we consider that it would be an excessive treatment, the

possibility that the prankster will (ii) download the voice of the prankster to be able to go to

said recording as many times as you want and be able to broadcast it without any restriction, so

in addition (iii) there would be a lack of security measures that would prevent said subsequent treatment by the

joker. If what MIRACLIA intends, with a purely commercial interest, is to charge for

play a joke, such treatment could be done without the need to record the voice or the

telephone number, and without having to give the prankster the absolute and unlimited possibility of

download the voice of the overwhelmed person to your terminal in order to be able to broadcast it later without

any limitation. Therefore, the second requirement regarding non-excessive use would not exist.

or necessary.

Thirdly, with regard to weighting or weighting, that is, not

prevail the fundamental rights and freedoms of the interested party in the protection of the

data, the CJEU has understood (Rigas Satskime judgment) that it depends on the circumstances

of the particular case in question.

In relation to this weighting, the Working Group of art. 29 of the Directive

95/46 issued Opinion 06/2014 on the concept of legitimate interest of the person responsible for the

treatment. Said Group, in its Opinion, states that

"…such an examination requires a full consideration of a number of factors, in order to

ensure that the interests and fundamental rights of citizens are duly taken into account

affected. At the same time, it is a modular test, which can vary from simple to

complex, and need not be unduly burdensome.

The factors to be considered when carrying out such a balancing test

will understand:

- the nature and source of the legitimate interest, and whether the data processing is necessary for the

exercise of a fundamental right, is otherwise in the public interest or benefits from the

recognition of the affected community;

- the repercussion for the interested party and their reasonable expectations about what will happen with their data,

as well as the nature of the data and the way in which they are processed;

- the additional guarantees that could limit an undue impact on the interested party, such as the

data minimization, privacy protection technologies, increased

transparency, the general and unconditional right of voluntary exclusion and the portability of the

data.

(a) As to the nature and source of the alleged legitimate interest, this is an interest of

commercial nature, as has already been shown. The TS, in its sentence STS

1921/2017, of May 5, 2017, Rec. 407/2016, has already made it clear that it cannot

prevail the interest of gas marketers over the interest of consumers



holders of electricity supply contracts, given that the latter have a right

fundamental against a merely commercial interest, so that the person, the consumer

in this case, it has the legal power to impose on third parties the duty to refrain from any

interference in their intimate sphere and the prohibition to make use of the and known, (with

citation of the sentences of the TC 73/1982, 89/1987, 231/1988, 134/1999 and 115/2000).

(b) It should be added, continuing with the list of recommended requirements for weighting, that

the data processing that the appellant intends to carry out is not at all necessary

for the exercise of a fundamental right, so it will have to decline in the face of the

need for protection of their fundamental right by the interested parties.

(c) Nor can it be considered that the processing of personal data proposed by

MIRACLIA results from the public interest or that benefit from the recognition of the affected community.

(d) Regarding the reasonable expectations for the interested party regarding the use of his personal data and the repercussions for him, it is enough to mention that with the treatment of personal data that the appellant intends to carry out, the interested party loses all power of disposition on them, since the data is registered by system, before being able to give their consent or even to be informed, so the prankster-user will be able to do use of the personal data of the abromado, his voice, downloading it in his own terminal and subsequently disseminating it among other third parties whenever and however you want, and this with regardless of whether the interested-overwhelmed person can make use of a hypothetical right to blocking or deleting your data against MIRACLIA, which, as it can easily observed from the mechanics of the application of the system, it will not be effective in any case if the prankster has already downloaded the voice to his terminal, since his broadcast is no longer It would depend on that entity.

(e) Regarding the nature of the data, we consider that the voice is a data particularly sensitive. And it is because we all know that the voice identifies univocally to a subject among a more or less extensive community. But the older abundance, the voice can also be considered sensitive data in another sense, and it is that the RGPD allows to consider the voice as a biometric data, as long as it is apply, or may be applied, techniques aimed at allowing the univocal identification of a natural person (art. 9.1 RGPD). It does not appear that the data processing that the responsible intends to carry out with the application ***APPLICATION.1 is addressed to apply treatment techniques to the voice that convert it into a biometric data, but Although that is not the purpose of the data processing carried out by the person in charge, it does not there is no doubt that the voice can constitute the raw material, the raw data, from the which a technique could be applied so that said personal data, the voice, turns out to be

a biometric data. As the Supreme Court has had occasion to consider in the aforementioned

previously sentence STS 1921/2017, of May 5, 2017, Rec. 407/2016, the criterion

of "risk" is a criterion to be taken into account when personal data, together with others, and with

violation of the principle of information or access, may lead to the identification of the

interested.

(f) Regarding the last of the weighting criteria mentioned, namely, the guarantees

that could limit an undue impact on the interested party, such as the

data minimization, privacy protection technologies, increased

transparency,

We believe that it is absolutely necessary to increase the



transparency in the sense of providing the possible overwhelmed, in advance of the

recording of your voice or your telephone, all the circumstances referred to in the article

13 GDPR. And in addition to that, the fact of recording the voice of the overwhelmed in the systems of the

appellant is considered excessive, in the sense of art. 5.1.c) GDPR.

In short, and to finish with this point, it does not result from data processing

carried out by MIRACLIA that concurs, beyond its own commercial interest,

no circumstance that justifies the recording of the voice of the overwhelmed using

as legal basis for the treatment the legitimate interest of article 7.f) of the Directive. The

processing of personal data carried out by MIRACLIA is not necessary for the satisfaction

of a legitimate interest, and in addition the legitimate interest of the appellant does not prevail against the

fundamental rights and freedoms of the interested party in the protection of their data

personal.

Consequently, it cannot be considered that the processing of personal data that

carried out by MIRACLIA is protected by the legitimate interest provided for in article 6.1.f) of the

GDPR. Nor does the interested party give their consent for said data processing,

which is unlawful, moreover, since the right to information has been completely dispensed with

of the interested party in the terms provided in the personal data protection regulations.

In accordance with the foregoing, the aforementioned facts entail a violation of the

article 6 of the RGPD, which gives rise to the application of the corrective powers that article

58 of the RGPD grants the Spanish Data Protection Agency.

IX

In its arguments to the motion for a resolution, MIRACLIA points out that the

arguments contained in the above legal grounds are not valid for

"*** APPLICATION.1", which is in a technical and data processing scenario

different from the one presented in previous actions of the Agency and the ordinary Justice.

For the present case, according to MIRACLIA, "***APPLICATION.1" conforms to the definition of

number-based interpersonal electronic communications services, defined

in article 2, sections 5 and 6, of Directive (EU) 2018/1972, which establishes the

European Electronic Communications Code (consolidated version).

Based on this consideration, MIRACLIA understands that it only intervened by facilitating

the necessary means to provide the service that the user has contracted, the only

data controller of the person receiving the prank call; that

the conversation that takes place for the provision of the service is personal or domestic, in the

insofar as the object of the service is to establish a communication initiated by the

joker, MIRACLIA limiting itself to facilitating the means for transmission; and what does not do

processing of prank call recipient data beyond compliance

of the conservation obligations imposed by Law 25/2007, on data conservation

relating to electronic communications and public communications networks.

For the same reason, MIRACLIA understands that it is not obliged to facilitate the

information referred to in the RGPD, as the provisions of Recital

173 and article 95 of said Regulation, in relation to Directive 2002/58/EC, on the

privacy and electronic communications. According to said article, the RGPD will not impose



additional obligations to natural or legal persons in terms of treatment in the

framework of the provision of public services of electronic communications in networks

public communications of the Union in areas in which they are subject to obligations

with the same objective established in Directive 2002/58/CE, and, in accordance

with this Directive, electronic communications services cannot be required to

based on public numbering resources that identify the manager of the

call or the owner of the platform or indicate where to obtain information about the

call or about the exercise of rights. Likewise, the right of the user must be respected

of the service not to identify themselves and to personally record the call.

These allegations must be rejected, as there is still no domestic law

no provision that transposes Directive (EU) 2018/1972, whose term of

transposition has not yet passed. This being so, it cannot be said that the activity that

developed through the application "***APPLICATION.1" fits into a category of services

of electronic communications that, at this time, does not exist in our legal system

legal.

On the other hand, article 95 of the RGPD, which

prohibits the imposition of “additional obligations on natural or legal persons in matter of treatment within the framework of the provision of public services of electronic communications on public communication networks in the Union in areas in those that are subject to specific obligations with the same objective established in the Directive 2002/58/EC”, which is not among the Directives that will be repealed by the Directive (EU) 2018/1972 with effect from 12/21/2020. This act is not referred to Directive 2002/58/CE nor does it imply the imposition of specific obligations with the same objective intended by this Directive

In any case, it should be added that MIRACLIA bases these allegations on the result of the audit carried out on the application “***APPLICATION.1” by an engineer of telecommunications in July 2020, well after the period analyzed by the Services of Inspection of this Agency. Although the responsible entity affirms that the version of the audited application corresponds to the current version at the time they were formulated complaints, there is no evidence to prove it. Furthermore, this allegation whatever was raised in his arguments at the opening of the procedure and supposes an approach different from the position that MIRACLIA has maintained during the previous phases, in which showed its willingness to correct some of the deficiencies revealed and defended the legitimate interest of the entity for the processing of data that it performs.

In addition, it starts from premises and takes for granted facts that cannot be accepted, mainly those related to the existence of a conversation between a user of “***APPLICATION.1”, who starts it, and a third party. It is stated that “the person who initiates the conversation must be the user who contracts the service ***APPLICATION.1” and that “once the connection is established between the user of ***APPLICATION.1 and the recipient of the conversation allows the direct exchange of interpersonal information through electronic communications networks between the two. However, as has been accredited, the user of the application simply schedules a call, in which no

participates, which is carried out from the MIRACLIA systems with the purpose of reproducing the recipient a locution (the one corresponding to the joke selected by the user), so that neither does that call put two people in communication nor does any "direct interpersonal information exchange". If there is a call between the



user and the recipient of the prank, that conversation would in no case take place with the intermediation of "***APPLICATION.1".

In the same way, it cannot be admitted that the user of "***APPLICATION.1" is the who decides to record the content of the message that he himself edits. The call joke remains in any case in the MIRACLIA systems, without being necessary to this the participation of the user of "***APPLICATION.1", which is limited to using the means provided by the entity itself to access the audio file generated by the system, without said user takes any action to edit your content.

With regard to this issue, the approach set out in the audit report provided by MIRACLIA, according to which the service qualification of electronic communications that is included in the Conditions of Use of the application implies an implicit acknowledgment of the nature of the service (in Annex II to the report of audit, the following is literally affirmed: "In the conditions of use of the application ***APPLICATION.1 in article 6 it is indicated that "as with any service of telecommunications, it is illegal to use the services of ***APPLICATION.1 for the purpose to harass or harm anyone." There is therefore a contractual declaration that ***APPLICATION.1 is a service subject to telecommunications regulation and, therefore, a

implicit acknowledgment that it is an electronic communications service in

Such case").

It is obvious that the position that MIRACLIA occupies in everything related to the

of the application “***APPLICATION.1” cannot be determined by an agreement between

individuals or a contractual statement, but by the legal determinations that result

applicable.

It can even be said that the aforementioned allegations must be dismissed.

even if we consider the provisions of the European Communications Code

Electronic, which defines interpersonal communications services including in this

concept of the transport of signals and other types of services that allow communication.

It distinguishes “three types of services that may partially overlap, namely:

internet access defined in article 2, point 2, of Regulation (EU) 2015/2120 of the

European Parliament and of the Council (1); interpersonal communications services, such as

defined in this Directive, and services consisting wholly or mainly of the

transport of signals” (Recital 15 of Directive (EU) 2018/1972, by which

establishes the European Code of Electronic Communications).

In accordance with its article 2 "Definitions", for the purposes of the aforementioned Directive:

<< shall be understood as:

4) “electronic communications service”: the service generally provided in exchange for a

remuneration through electronic communications networks, which includes, with the exception of

services providing content transmitted via communications networks and services

or exercise editorial control over them, the following types of services:

a) the “internet access service”, understood according to the definition of point 2) of paragraph

second of article 2 of Regulation (EU) 2015/2120;

a) the “interpersonal communications service”, and

b) services consisting wholly or principally of the transport of signals, such as

are the transmission services used for the provision of machine-to-machine services

and for broadcasting;

5) “interpersonal communications service”: the service generally provided in exchange for a

remuneration that allows a direct, interpersonal and interactive exchange of information through

of electronic communication networks between a finite number of people, in which the initiator of

communication or participant in it determines the recipient or recipients and does not include services that

allow interpersonal and interactive communication as a mere secondary possibility that goes

intrinsically linked to another service;

6) “number-based interpersonal communications service”: communications service

interpersonal networks that either connect or enable communications with public numbering resources

assigned, that is, of a number or numbers of the national or international numbering plans, or

allows communication with a number or numbers of the national numbering plans or

international;>>.

In relation to these definitions, what is stated in the

Recitals 17 and 18 of the same Directive:

(17) Interpersonal communications services are services that allow the exchange

interpersonal and interactive information and services such as voice calls

between two people, as well as all kinds of emails, services of

messaging or group chats. Interpersonal communications services only cover the

communications between a finite number, that is to say, potentially not unlimited, of natural persons, who

is determined by the sender of the communication. The communications in which they intervene

Legal persons should fall within the scope of the definition when the persons
natural persons act on behalf of those legal persons or intervene at least on one side of the
communication. Interactive communication assumes that the service allows the receiver of the
information respond. Services that do not meet these requirements, such as linear broadcasting,
video on demand, websites, social networks, blogs or the exchange of information between
machines, should not be considered interpersonal communications services. In
In exceptional circumstances, a service should not be considered a communications service
interpersonal if the interpersonal and interactive communication device is a characteristic
minor and purely auxiliary to another service and, for objective technical reasons, cannot be used without
said main service and its integration is not a means to circumvent the applicability of the rules that
regulate interpersonal communications services. As elements for the
exclusion from the definition, the terms "minor" and "purely auxiliary" should be interpreted
restrictive and from an objective end-user perspective. A communications feature
interpersonal relationships can be considered minor when their objective usefulness to an end user is very
limited and when, in reality, it is hardly used by end users. An example of a
characteristic that can be considered falls outside the scope of the definition of
Interpersonal communications services could be, in principle, a communication channel of a
online game, depending on the characteristics of the communication device of the service.
(18) The interpersonal communications services that use numbers of a national plan and
international numbering services connect with publicly assigned numbering resources. Those
number-based interpersonal communications services encompass both services in
which end user numbers are assigned to ensure end-to-end connectivity.
such as services that enable end users to come into contact with
people to whom those numbers have been assigned. The mere use of
a number as an identifier is equivalent to the use of a number to connect with
publicly assigned numbers and therefore should not be considered sufficient by itself to

qualify a service as a number-based interpersonal communications service. The



number-independent interpersonal communications services should only be

subject to obligations when the public interest requires the application of regulatory obligations

specific to all types of interpersonal communications services, regardless of

that use numbers to provide their service. It is justified to treat differently

number-based interpersonal communications services, as they participate in a

publicly guaranteed interoperable ecosystem and therefore also benefit from it.

Therefore, an interpersonal electronic communications service based on

numbering must allow a direct, interpersonal and interactive exchange of information

between people, without this interpersonal and interactive communication being included in the

service in question as a mere secondary possibility.

Consequently, MIRACLIA is not a provider of networks and communications

electronic communications or provide electronic communications services.

On the other hand, due to the exposed circumstances, this Agency understands that it is not

applicable to this case the doctrine of the Constitutional Court alleged by

MIRACLIA, which admits the recording of a conversation between people by one of the

participants. Nor does this Agency consider that this assumption raises

any controversy that affects the right to freedom of expression of citizens.

Also in his arguments to the motion for a resolution, MIRACLIA points out as

Proven Fact 1 is false, in which it is indicated that said entity is the owner of a

mobile application called "***APPLICATION.1", stating that it is a service to the

accessed via a mobile app. However, in relation to this

question, we refer to the many references that the document "Terms and

Conditions of Use of the Service" contains about the application "***APPLICATION.1" (eg:

"Service definition: ***APPLICATION.1 is an application…").

And he also considers the reference to the lodging of the jokes on a site to be erroneous.

public, since access to the audio is done through a private URL to which only

The sender of the joke and the recipient of the same have access, if the former so wishes.

Well, this Agency understands that what is indicated in Proven Fact 4 is not contrary

to what is indicated by MIRACLIA when it indicates that there is no "a platform in which

publish the jokes made so that any third party can access them, but the

recordings of the pranks are hosted on a public site, which makes it possible to

access to them through the link to the audio file, which can be broadcast

indiscriminately by the prankster user."

In relation to what is stated in Proven Fact 5, it is alleged that the link to which

accessed the Inspection Services of the Agency to verify that

"*** APPLICATION.1" operates in other countries of the European Economic Area corresponds to

a pre-production platform that has never worked. However, as stated in

Inspection Diligence, access was made from the offices of the Agency itself to

information that was in production on that day, available to any third party

network user, that is, publicly accessible information. Inspection Services do not

have made no access to MIRACLIA systems under development. In any case, this

entity does not deny the information contained in the aforementioned Proven Fact, on the

operation of the application "***APPLICATION.1" in the countries indicated and the

availability to the public of the terms and conditions of use in the languages outlined.

Regarding the claims that are outlined in the Background,

MIRACLIA repeatedly warns that they should not have been admitted for processing, taking into account that the respective claimants did not previously address the entity exercising the rights recognized by the personal data protection regulations.

In this regard, on the one hand, it should be noted that this Agency, using the powers and prerogatives attributed to it, determined as the object of the proceedings the global analysis of the application "***APPLICATION.1" from the point of view of the regulations of personal data protection and in relation to the people who receive the calls joke, regardless of the specific incidences of the claims raised, which served to motivate the start of the appropriate investigations in relation to with the treatment of the personal data of the people who receive the calls of joke, which coincides with the object of the claims; and, on the other hand, that the exercise of those rights is not established as a necessary presupposition to be able to formulate a claim before this Agency. The decision whether or not to make this claim or the The use of any other means to defend their rights is exclusive to the claimant. In In any case, it is considered convenient to point out that the decision that is adopted results from the facts declared proven, without any scope having been attributed to the questions highlighted by MIRACLIA in relation to the demonstrations carried out by the complainants about sending the recording by whatsapp, making calls other than the prank call, the sending of emails or the attention given by MIRACLIA to requests to exercise rights.

Unlike the present case, the precedent cited by MIRACLIA, in which deals with the case of a person who received a prank call from a radio station,

refers to a claim of protection of rights for the non-attention of the request for

cancellation of data that had previously been raised before the person in charge, and as such was

processed by this Agency.

Finally, MIRACLIA requests a face-to-face hearing procedure to clarify before

instructors/inspectors of the Agency the exposed points and warns that, in case of

not see their interests served, reserves the right to go to other higher instances

and/or judicial in Spain and in Europe. This hearing is not provided for in the regulations.

applicable procedure, so that it is not obligatory to carry out this procedure nor does it harm the

right of defense of the interested entity, which, obviously, will have the

possibility of challenging the resolution in all the ways provided for in the aforementioned regulations.

X

In the event that there is an infringement of the provisions of the RGPD, between the

corrective powers available to the Spanish Data Protection Agency, such as

control authority, article 58.2 of said Regulation contemplates the following:

“2 Each supervisory authority shall have all of the following corrective powers

listed below:

(…)

b) sanction any person responsible or in charge of the treatment with a warning when the

treatment operations have violated the provisions of this Regulation;”

(...)



d) order the person in charge or in charge of the treatment that the treatment operations

comply with the provisions of this Regulation, where appropriate, in a

certain manner and within a specified period;

(…)

i) impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;".

According to the provisions of article 83.2 of the RGPD, the measure provided for in letter d)

above is compatible with the sanction consisting of an administrative fine.

eleventh

In the present case, the processing of personal data that

MIRACLIA entity performs without having previously informed the owner of the data and without

legitimacy for it.

The interested party does not even know that their personal data is being processed

by this entity, which uses an application designed to use personal data

provided by a third party and by the interested party. The application is created with a purpose

that requires the processing of personal data. Thanks to the application is subjected to

treatment the telephone line to which the communication is sent, the recording and reproduction of the

conversation held by the interlocutors.

In accordance with the findings obtained, it is considered that the facts

exposed could breach the principle of transparency established in articles 12, 13 and

14 of the RGPD, as well as the principle of legality of the treatment regulated in article 6 of the

RGPD, which, if confirmed, could lead to the commission of two infractions

typified in article 83.5 of the RGPD, which under the heading "General conditions for the

imposition of administrative fines" provides the following:

"Infractions of the following provisions will be sanctioned, in accordance with section 2, with

administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, a

amount equivalent to a maximum of 4% of the total annual global turnover for the year

previous financial statement, opting for the highest amount:

a) the basic principles for processing, including the conditions for consent under

of articles 5, 6, 7 and 9;

b) the rights of the interested parties pursuant to articles 12 to 22; (…)".

In this regard, the LOPDGDD, in its article 71 establishes that "They constitute

infractions the acts and behaviors referred to in sections 4, 5 and 6 of article 83

of Regulation (EU) 2016/679, as well as those that are contrary to this law

organic".

For the purposes of the limitation period, article 72 of the LOPDGDD indicates:

"Article 72. Infractions considered very serious.

1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679, they are considered very

serious and will prescribe after three years the infractions that suppose a substantial violation of the



articles mentioned therein and, in particular, the following:

(…)

b) The processing of personal data without the concurrence of any of the conditions of legality of the

treatment established in article 6 of Regulation (EU) 2016/679.

(…)

h) The omission of the duty to inform the affected party about the processing of their personal data

in accordance with the provisions of articles 13 and 14 of Regulation (EU) 2016/679 and 12 of this Law

Organic".

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

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

"1. Each control authority will guarantee that the imposition of administrative fines in accordance with

to this article for the infractions of this Regulation indicated in sections 4, 9 and 6

are in each individual case effective, proportionate and dissuasive.

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

as an additional or substitute for the measures referred to in article 58, paragraph 2, letters a) to h)

and j). When deciding the imposition of an administrative fine and its amount in each individual case,

shall take due account of:

a) the nature, seriousness and duration of the infringement, 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 person in charge or in charge of the treatment to mitigate the damages and

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, taking into account the

technical or organizational measures they have applied under 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 potential adverse effects of the breach;

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 if the

The person responsible or the person in charge notified the infringement and, if so, to what extent;

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

against the person in charge or the person in charge in question in relation to the same matter, the

compliance with said measures;

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

approved under 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 the

infringement."

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

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679

will be applied taking into account the graduation criteria established in section 2 of the aforementioned

Article.

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

be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the processing of personal data.



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

d) The possibility that the conduct of the affected party could have led to the commission of the offence.

e) The existence of a merger by absorption process subsequent to the commission of the infraction, which does not

can be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when not mandatory, a data protection delegate.

h) Submission by the person in charge or person in charge, on a voluntary basis, to mechanisms of

alternative resolution of conflicts, in those cases in which there are controversies between

those and anyone interested."

In accordance with the precepts transcribed, in order to set the amount of the

sanctions of a fine to be imposed in this case on the defendant, as responsible for

infringements typified in article 83.5.a) and b) of the RGPD, it is appropriate to graduate the fine that

It would be appropriate to impose for each of the imputed infractions.

It is estimated that they concur as aggravating circumstances, applicable to the two infractions.

of the RGPD for which MIRACLIA is responsible, the following factors that reveal a

Greater unlawfulness and/or culpability in the conduct of the entity:

. The nature, seriousness and duration of the offence, taking into account the nature,

scope or purpose of the processing operations in question: the seriousness of the

infringement is determined by the processing operations carried out

MIRACLIA, which include the collection of personal data to make them available to

third parties, offering them, in addition, functionalities or tools for the dissemination of said

personal data, despite the fact that its treatment is contrary to the RGPD. The duration of the

infringement, considering that it is linked to the proper functioning of the application

"***APPLICATION.1" is determined by the period of exploitation of said application.

. The intentionality or negligence appreciated in the commission of the infraction: this

This circumstance results from the design of the application itself, which has not foreseen in any way

compliance with personal data protection regulations. It's an aggravating

especially significant because the claimed, without any doubt, knew the

defects appreciated by this Agency in the operation of the application from

several precedents, in which he was sanctioned for the infringement of the principle of

consent. MIRACLIA is not unaware that its conduct entails a violation of the RGPD and

decided to go ahead with it.

. The continuous nature of the infringement: the result of the uninterrupted exploitation of the

application “***APPLICATION.1”.

. Linking the activity of the offender with the performance of data processing

personal and benefits obtained as a result of the commission of the infraction: all

the operations that constitute the commercial or mercantile activity carried out by the

claimed involve personal data processing operations, and all of them affected

for the same regulatory breaches. Thus, all the benefits of this business

are the result and consequence of the permanent infringement of data protection regulations

for which the respondent is responsible

. The volume of data and processing that constitutes the object of the file; and number of

interested parties: it is taken into account that the defects appreciated in the data processing

affect everyone who receives a prank call using the app



“***APPLICATION.1”.

. The nature of the damages caused to the interested persons or to third parties:

The damages that may arise from the processing of the data and its dissemination are

unpredictable, without MIRACLIA having taken any precautions in this regard.

. The imputed entity does not have adequate procedures in place for action in the

collection and processing of personal data, so that the infringement is not

consequence of an anomaly in the operation of said procedures but a

defect of the personal data management system designed by the person in charge.

Considering the exposed factors, the initial valuation of the fine included in the

opening agreement amounted to 50,000 euros per house one of the offenses charged.

However, the company has requested in its statement of arguments a reduction of that fine, since it represents 25% of its turnover, which amounted to 476,000 euros in 2018, in which there were losses.

The financial information available regarding MIRACLIA corresponds to the year 2018, last fiscal year presented. There is a turnover figure for that financial year 475,823 euros and a result for the year of -7,364 euros. Also, it is verified that It is a microenterprise, with 2 employees. According to the information in the Central Mercantile Registry, the "Subscribed Capital" amounts to 6,000 euros

Considering this circumstance, it is deemed appropriate to propose the imposition of a fine amounting to 20,000 euros for each of the offenses committed [infringement of the principle of transparency due to non-compliance with the provisions of the articles 13 and 14 of the RGPD, typified in article 83.5.b) and classified as very serious to effects of prescription in article 72.h) of the LOPDGDD; and infringement for non-compliance of what is established in article 6 of the RGPD, typified in article 83.5.a) and qualified as very serious for prescription purposes in article 72.1.b) of the LOPDGDD].

XII

In accordance with the provisions of article 58.2.d) of the RGPD, each authority of control may “order the person responsible 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…”.

In this case, considering the circumstances expressed in relation to the Appreciated defects in the operation of the application "***APPLICATION.1", from the point of view of data protection regulations, it is appropriate to require MIRACLIA to that, in the term that is determined, adapts to the personal data protection regulations the treatment operations it carries out, the information offered to its clients and the procedure by which they give their consent for the collection and

treatment of your personal data; establishing, in addition, mechanisms that allow

prove that the interested party has effectively accessed the information offered and that

They gave their consent for the collection and processing of personal data. All

this with the scope and in the sense expressed in the Foundations of Law of the



this resolution.

In those cases in which the interested party was not duly informed about

the circumstances regulated in articles 13 and 14 of the RGPD or the interested party had not

given their consent, MIRACLIA will not be able to carry out the collection and treatment of

Personal information.

On the other hand, it is appropriate for the MIRACLIA entity to cease the illicit use of the

personal data contained in their information systems relating to

Interested parties who have not given their informed consent to do so

These measures will be applicable in all the countries of the Economic Area

Europe in which MIRACLIA operates through the application "***APPLICATION.1" and

with respect to interested parties residing in said countries.

It is warned that not meeting the requirements of this organization may be

considered as a serious administrative infraction by “not cooperating with the Authority of

control” before the requests made, being able to be valued such conduct at the time of

the opening of an administrative sanctioning procedure with a pecuniary fine.

Therefore, in accordance with the foregoing, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: Penalize the entity MIRACLIA TELECOMUNICACIONES, S.L., for a infringement of articles 13 and 14 of the RGPD, typified in article 83.5.b) and qualified as very serious for prescription purposes in article 72.h) of the LOPDGDD, with a fine amounting to 20,000 euros (twenty thousand euros).

SECOND: Penalize the entity MIRACLIA TELECOMUNICACIONES, S.L., for a infringement of article 6 of the RGPD, typified in article 83.5.a) and qualified as very serious for prescription purposes in article 72.1.b) of the LOPDGDD, with a fine for amount of 20,000 euros (twenty thousand euros).

THIRD: Require the entity MIRACLIA TELECOMUNICACIONES, S.L so that, in the period of three months, adapt to the personal data protection regulations the treatment operations that it carries out, the information offered to its clients and the procedure by which they must give their consent for the collection and treatment of your personal data, with the scope expressed in the Basis of Law XII. Such adaptation must be implemented equally in all the countries of the Space European Economic in which MIRACLIA operates through the application "***APPLICATION.1".

FOURTH: NOTIFY this resolution to MIRACLIA TELECOMUNICACIONES, S.L.

FIFTH: Warn the sanctioned person that he must make the imposed sanction effective once This resolution is executive, in accordance with the provisions of art. 98.1.b) of the Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations (hereinafter LPACAP), within the established voluntary payment period in art. 68 of the General Collection Regulations, approved by Royal Decree

939/2005, of July 29, in relation to art. 62 of Law 58/2003, of December 17,

by entering, indicating the NIF of the sanctioned person and the number of the procedure that

appears at the top of this document, in the restricted account number ES00 0000

0000 0000 0000 0000, opened on behalf of the Spanish Agency for Data Protection in

the banking entity CAIXABANK, S.A.. Otherwise, it will be collected in

executive period.

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

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

will be until the 20th day of the following or immediately following business month, and if it is between the

16th and last days 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 LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the Director of

the Spanish Agency for Data Protection within a 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 fourth additional provision

of Law 29/1998, of July 13, regulating the Contentious-administrative Jurisdiction,

within two months from the day following the notification of this act,

according to the provisions of 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 Electronic Registry

of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the

remaining records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1.

You must also transfer to the Agency the documentation that proves the filing

effectiveness of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the day

following the notification of this resolution, it would end the suspension

precautionary

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es