agencia española protección datos

## Final Decision

**Details of case**

| | |
|---|---|
| National file number | PS/00416/2019 |
| IMI Case Register number | 72167 |
| Controller | MIRACLIA TELECOMUNICACIONES, S.L. |
| Complainant | [redacted] and [redacted] |
| Legal references | 6, 13 y 14 GDPR |
| Administrative fine / penalty imposed | 40.000 € and requirement of adaptation to data protection regulations |

1054-0319

**Summary of the complaint**

The complainant filed a complaint with the Spain-SA against MIRACLIA // The complaint lodged by [redacted] has been transmitted to the Spain-SA according to provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint claim the use of personal data to make a joke using the "Juasapp" application, by means of a telephone call to his mobile line 639610479 in which a person pretended to be a police officer, which took place on 09/01 / 2018. For this reason, he denounces the recording made without his knowledge or consent, the dissemination of said recording to third parties, also without his consent, and that the call is made from a hidden number. He adds that the line enabled as a contact by that company has an additional rate, which entails a cost for the interested party who intends to contact it. He states that he has a copy of the recording, which was provided to him by the person who used the services of MIRACLIA and requests that his data be cancelled, as well as the opening of a sanctioning procedure.

This claim was transferred to the entity MIRACLIA. In response to what was stated by the claimant, MIRACLIA informs this Agency that the joke to which the claimant refers is not included in the "Juasapp" application, in whose catalog of jokes there is none that has to do with police officers.

Regarding the processing of personal data, it indicates that it does not store data of the subject subjected to the joke (hereinafter, also, interested party or person who receives the joke call): neither recordings nor telephone, which will be on the joker's mobile device (hereinafter, also, user of the application or person who orders the prank call); limiting itself to providing a service to the user of the application (the joker) who chooses the joke, enters the recipient's phone number and, after accepting the terms and conditions, generates the recording. MIRACLIA, therefore, has no way of knowing if the claimant has received a joke from "Juasapp" (it warns that there are other similar applications), and it can only block the telephone line number of the person who have received the joke call, even without knowing if he has actually received the joke, or delete the URL of the recording if they had it, which does not happen in this case as it was not been provided by [redacted].

According to MIRACLIA, it is the joker who can erase the recording, so the claimant's request must be addressed to him. The entity's action, which does not identify the abused people, consists of preventing the recipient of the joke from receiving more calls in the future, blocking the phone, or proceeding to delete the recording using the URL of the joke, which does not carry any associated telephone, and provided that the joker has not previously done so.

The user of the application or joker is warned on two occasions about the responsibility that the recording entails.

Finally, MIRACLIA informs that since the full application of 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 already The Free Circulation of these Data (hereinafter RGPD), has modified its operation in order not to keep any type of data, leaving these on the users' phones, being impossible to identify the person who receives the joke call. In the event that the latter, the person who receives the joke call, provide his line number, they could be blocked so that they do not receive calls in the future.

On 07/04/2019, a claim filed by [redacted] (hereinafter claimant 2), against the entity MIRACLIA, noted, like claimant 1, that it has been the subject of a joke (thanks for her vote to Vox) that was been recorded and disseminated by social networks with the mention of her name, carried out using the application "Juasapp" (provides the link to the audio object of the complaint - "http: // juasapp .mobi: 8080 / ... ", which allows access to the audio corresponding to the call). She request the removal of her mobile phone line number on which she received the call from the database of the responsible company and the removal of the audio from the network. She also denounces that xenophobic messages are made from the supposed "association of friends of Vox".

**Competence**

Pursuant to Article 56 (1), paragraphs 2 and 4 of Article 58, and Article 60 of GDPR, and in accordance with Article 48 (1) and 64 of the Constitutional Act 3/2018 of 5 December on Personal Data Protection, the Chair of the Spain-SA shall have competence to

ADOPT THIS FINAL DECISION

**Investigation by Spain-SA**

The Spain-SA has conducted an investigation to determine how personal data is processed to make jokes.

1. Made a request for information to MIRACLIA on various aspects, on 06/25/2019 a letter from said company was received at this Agency in which it makes the following statements:

a) At the end of the joke call, the receiver listens to an announcement offering him the possibility of not allowing the generation of the file with the recording of the joke. The locution is as follows:

"A friend of yours has played a joke on you. In case you do not want your friend to listen, download or broadcast the joke, or in case you do not want to receive more jokes, press 5 on your keyboard after the signal. Beeep "

They add that additionally, the joke can be deleted by knowing the url of the joke recording and sending an email to apps@miraclia.com indicating that url.

b) Among other technical aspects, they indicate that, once the prank is programmed, the call is initiated from the Voice over IP servers of MIRACLIA on the specified date and time.

The joker user downloads the application and accepts its terms and conditions. At that time, a user profile is generated to use a Voice over IP service and a number is assigned to him, which is rented to you while you are a user of the application and make each call. To use the application, choose a joke from the catalog and enter the phone number of the joke recipient and program a date and time, and the Voice over IP call leaves the cloud servers at that time that the user has programmed the joke.

If the joking user selects to record the call (and the receiver does not choose the option that it should not be recorded), an audio file will be generated with the content of the joke call . The generated audio file is available at a URL to which only the joker user of the application has access and only the joker on his device where he has installed the application has that content associated with the phone number of the recipient of the call, since Juasapp's servers do not store any personal data of the recipient of the call.

c) In the terms and conditions of use of the application, joking users are informed that the company could delete their profiles (including content / 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 into the application since the last claim, an inspector installed the "Juasapp" application on his mobile terminal. The application consists of 3 tabs: "List" (of available jokes), "Examples" and "My jokes". This last tab is where the jokes made by the joker will be saved if they are not deleted.

It is verified that the list of available jokes includes jokes related to claimant 1 and claimant 2.

3. On September 6, 9 and 12, 2019, the Agency's Inspection Services carried out

tests consisting of downloading the "Juasapp" application on a mobile terminal and proceeding to use it. As a result of these tests, the findings outlined in the Second Proven Fact were obtained.

4. It has been found that the website "juasapp.es" offers a free and immediate system to include a phone number in the list of blocked phones. According to MIRACLIA's statement, the phone number is stored encrypted in its systems.

A test was carried out by registering the telephone number corresponding to a second SIM of the inspector's terminal, and then a prank was attempted on this telephone number. The application did not allow the execution of the joke.

5. Regarding the issue of the dissemination of the joke, which is present in the claims, it must be clarified that MIRACLIA does not have any public site where they are published or any platform for the dissemination of jokes. The jokes can only be spread by the joker user by sending the link to the audio file: in the list of jokes made by the joker, next to each of the jokes not eliminated by the receiver of the joke following the indicated procedure, appears an icon to download the audio file of the recording of the phone 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 means that has been chosen to share it - this is the only time the joker knows the link to the audio file).

6. On 08/26/2019, the Inspection Services access the website "juasapp.es", at the URL corresponding to the recording of the joke made on the claimant 2. It is verified that using the right button They show different options, including playing and downloading the recording.

Operational tests of the "Juasapp" application carried out as a result of previous actions carried out by the Agency (file E / 02003/2018) have been incorporated into this investigation. Regarding the treatment by MIRACLIA of the personal data of the recipient of a joke, the conclusions of that previous investigation indicate the following:

I. Storage of the recipient's phone. The recipient's telephone number is stored in the claimed systems until the moment the call is made. Prank calls can be instant or scheduled by specifying execution date and time.

II. Recording the joke. It remains in the systems of the claimed one until the joker decides to eliminate it. If the recipient of the joke decides to exercise his right of deletion, he must know the web link to the joke. As a general rule the joke record will be deleter in a period of time of 6 months of non-use of the application by the user.

III. There are no other personal data of the addressee of the joke in the systems of the claimed person in addition to those reflected in the previous points I and II.

An a sanction proposal was sent to MIRACLIA, indicating that its action could be financially sanctioned, with a fine of 100,000 euros for infringement of articles 6 and 13-14 of the RGPD.

MIRACLIA submitted a brief of allegations in which the company requests the reduction of the penalty referred to in the agreement to initiate the procedure, taking into account the allegations made and the immediate measures adopted. It bases its request on the following considerations:

1. As a preliminary matter, the aforementioned entity warns that it has been the subject of several sanctioning procedures previously (due to the absence 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, the position of MIRACLIA in the personal relationship between joker and person who receives the joke call is discussed when facilitating 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, depending on the entity) , otherwise the fact of playing a joke would not be possible. It accompanies a copy of one of the appeals, which summarizes, according to MIRACLIA, its arguments.

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

MIRACLIA indicates that it only provides security to the process, but is not capable of identifying the abused or linking it to any other data; does not save the phone to which the joke is directed does not associate it with the audio file, which is encrypted with a code. It adds that it blocks the phone of the recipient of the joke when it requests not to receive them, it deletes the recording when it is requested and it does not have lists of telephone numbers of abomados, lists of recordings 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 events and, at most, enable means to request the removal of content . Nor does a company dedicated to sending surprise gifts have to ask the recipient for prior permission. Otherwise, the activity would not be possible.

2. Regarding the claim made by claimant 1, he reiterates that the joke he refers to does not appear in Juasapp's catalog of jokes.

Regarding the second claim, she states that the interested party did not go to the entity to request the deletion of her 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 the right could have been satisfied.

3. About the tests carried out by the inspector:

- The recording is not materialized in an audio file with its corresponding URL

until the user making the call confirms that he has accepted the Terms and Conditions for the second time and generates the audio file.

- The erasure of the jokes occurs with the sending of a DTMF tone during the call, which the operators must guarantee its operation. Unfortunately in the VoIP world (which is the technology with which operators provide the service of sending telephone calls from Juasapp's servers), this is not always the case depending on the route 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 in the same way. It is already a standard for the usability of smartphones.

- The phone number for programmed pranks is stuck with the call to be made. When this is done, it disappears from the systems. At no time is the phone number and the recording stored at the same time and place, which makes it impossible for there to be an association between both data. The recording file is generated when the joker accepts its generation, which only occurs when the call has ended and the abuser has not pressed the 5 key. If the joker does not accept the generation of the recording, there is no audio conversion in 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 processing.

It questions whether the information can be considered personal data, since MIRACLIA is unable to identify the abused in a simple way and without disproportionate means, based on the mobile phone number or voice files (STS 2484/2019: “a natural person it is not considered identifiable if such identification requires disproportionate deadlines or activities ”). In this case, the only one who can identify the joked person 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 telephone number was stored on the user's device and not on the entity's servers. Initially, the telephone number of the abbreviated person was stored to facilitate any request for information from the affected party, although, according to MIRACLIA, in an irreversible encryption with sha-2 algorithm, avoiding the use of the number for any action other than giving that support, since It could only be recovered if someone (ex: the person that received the joke call himself) facilitated it.

At the same time, an informative note on data processing was included at the end of the joke that, although it is true that the current phrase does not inform about everything required in article 14 of the RGPD, it does indicate how to oppose the treatment of data. data and its deletion (insists that it considers that it does not treat personal data, but, "ad cautelam", informs and offers guarantees).

Likewise, in the privacy policy inserted in the web and in the Terms and Conditions of the app, the following is reported:

*'Miraclia does not collect data from the recipients of the jokes. Miraclia's activity is to provide a means of telecommunications to enable the owner of the telephone downloading the app to choose a joke and to record it, with data relating to the recipient of the call stored on the user's own terminal without Miraclia retaining information on the recipient's telephone number. Miraclia provides a cloud storage service for the customer's audio files and at no time does it disseminate or share that information with anyone, as it is private information of the app user.'*

Moreover, in the context of the present proceedings, which were aware of the complaint made for the first time in relation to the information defects, it immediately remedied it by supplementing the information provided at the end of the conversation of the joke as follows:

That someone has spent a joke to pass a good story.

The Juasapp application owned by MIRACLIA TELECOMUNICACIONES, S.L.

— To object to such a joke reaching the bromist and to remove it, you can click on key 5.

— You have more information by clicking on key 1.

Clicking on key 1 provides the detailed explanation, also included on the website. Thus, of the information which it did not provide to the data subject, it has now included:

The identity of MIRACLIA

— the contact details of the Data Protection Officer

— The retention period

— The basis for locus standi

— The exercise of the full rights guaranteed by opposition and deletion rights (and also access rights when requested) are now formally specified.

This is a 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 FAQ section. Please provide the details of the information inserted in the "FAQ" section of the website:

*'12.- I do not want to receive more jokes. What do I do?*

*If you don't want anyone to know again, it is enough for you to touch my number in Bloquear and include the phone number. The phone number you enter will be blocked on the platforms so that nobody can send you a joke from this app (or of course no other action).The number is stored in the systems so that no one can retrieve that number for future use."*

*'16.- How can I erase a joke?*

*The jokes are erased by pushing the finger for a few seconds on the joke in question."*

It goes on to state that this does not mean that it is compatible with the infringement or with the penalty, but since this is not a matter which has been neglected in bad faith or with a view to evading compliance, it is immediately reinstated 'ad caution' with a view to remedying it.

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

Consent cannot be the legal basis for spending a joke because it would undermine the very fact of spending a joke or the surprise effect, as is also the case in many cases, such as the sending of flowers or the uploading of friends' photos to social media. In the latter case, the rights to erasure and objection are guaranteed, but the social network manager does not seek the consent of persons whose data are uploaded by other users.

MIRACLIA therefore defends the merits of the legitimate interest as a basis for standing under Article 6 (1) (f) GDPR.To this end, the required balancing test has been carried out, following the recommendations of the previous Article 29 Working Party.

What is more, it has been assessed that the legal basis is the performance of the contract between the user and MIRACLIA, but the person who receives the call is not a party to that contract.

To this end, we enclose a report justifying the legitimate interest as a basis for legitimising the processing of data and concluding that, a part from specific cases in which the person who receives the call is disturbed (which are testimonial cases), there is no risk to individuals because all security measures have been taken to ensure the security of the process, because it is ensured that the joke is erased if the person receiving the joke so requests, including telephone blocking.

Adds that the recording of a conversation between private individuals, where the person recorded is one of the participants in the conversation, is not unlawful, as stated by the Constitutional Court in its judgment of 29 November 1984, STC 11/1984, when it provides, inter alia, that 'Who recorded a conversation of others, irrespective of any other consideration, the right conferred by Article 18.3 of the Constitution is observed; on the other hand, a person who recorded a conversation with another person does not, by virtue of that fact alone, engage in conduct contrary to the aforementioned constitutional provision'.

In the case of Juasapp, the party issuing the call is aware of the recording of the call. The user could record the conversation with a recorder, the mobile phone itself or using apps recording the conversations. Instead, it uses a medium (Juasapp, which provides the service).Such a call occurs in a domestic environment between individuals who are not affected by data protection legislation.

If MIRACLIA, as it had done until recently and now repeats the recording, is providing greater guarantees (the person who receives the call of joke can choose to delete the recording, delete it subsequently, block his phone and prevent the user from spreading the joke).

5. The measures taken and the scale of the penalty

Highlights MIRACLIA that complaints submitted to the Agency represent a very small percentage (0.00002 %), compared to hundreds of users who have dealt with through different channels (web, post call term and customer service); whereas it has remedied the lack of information by completing the terms set out in Article 14 of the GDPR, but considers it essential that it did offer the possibility to object and to delete the

data; and that the proposed penalty would require the closure of the company, since it represents 25 % of its turnover, which amounted to EUR 476,000 in 2018, in which losses were incurred.

Calls for the proposed penalty to be revised downwards and, to that end, considers that the following should be taken into account:

.That we find ourselves in a leisure environment that does not harm the person called a joke, nor is his personal data misused.

.The only data at issue is the telephone number, which MIRACLIA does not keep and a recording which can only be generated and distributed by the user, which the entity cannot join as there is no file with the telephone and the recording.

.That the intention has always been to comply with the standard, ensure data security and minimise information.

.It has never failed to respond to requests for deletion.

.Until the present proceedings, the infringement has focused exclusively on the absence of consent, without the allegation of failure to comply with Article 14, which appears to be excessive in view of the fact that it has been informing and remedied it.

.It has shown readiness to cooperate with the Agency at all times and has provided the information requested.

.In the process under analysis, the person receiving the call is always chosen by the app user, who is responsible for making good use of the app.

.That the question of the legal basis of the processing is being discussed in the Supreme Court, which will decide whether the processing is anonymous for the entity, whether the security guarantees have been put in place and whether it is a means used by individuals in their private life.

MIRACLIA has provided a copy of one of the appeals lodged before the Tribunal Supremo (Supreme Court) in 2019, which is based on the following grounds:

1. Spending a joke through an application or a means in which the user is sovereign of the information provided is an act carried out at home or personal level and is therefore excluded from the protection of data protection rules.

2. Voice is not personal data if it does not allow the holder to be identified or if disproportionate efforts are needed to identify the data subject.

3. The legal basis for the processing of data (if this is considered to be personal data) by an application providing a means of leisure in the personal or domestic sphere of individuals is based on the legitimate interest.

.On 02/12/19 it was verified that using the link *http: //juasapp.mobi/web/change* the country in which the app operates can be changed. These countries include both the European Union (Austria, Belgium, Germany, etc.) and outside the European Union (China, the United States, Argentina, Brazil, South Korea, etc.).It is also verified that the terms and conditions of use of the service are written in English, Italian, French and German.

.On 03/12/2019, a new installation of the application was carried out, verifying that in the process it does not offer an option to shape another country or another language, although the terms and conditions of use of the service are written in English, Italian, French and German in the same way as those available via the Internet.

The acting inspection incorporates in the proceedings documents entitled 'Terms and conditions of use of the service' and 'Privacy policy'.The latter states:

*'1. INTRODUCTION*
*This privacy policy applies to the information we can obtain from or about you when using the JUASAPP mobile application (the "Mobile APP" or the "Service")".*

*'Miraclia does not collect data from the recipients of the jokes. Miraclia's activity is to provide a means of telecommunications to enable the owner of the telephone downloading the app to choose a joke and to record it, with data relating to the recipient of the call stored on the user's own terminal without Miraclia retaining information on the recipient's telephone number. Miraclia provides a cloud storage service for the customer's audio files and at no time does it disseminate or share that information with anyone, as it is private information of the app user.'*

The inspection services also carried out a test of downloading the app into a mobile terminal. It is checked that during the installation process the user receives the same text reproduced above about the non-collection of data from the recipients of the jokes and, among others, the following message:

*'Please read these Legal Terms and Conditions in detail and please accept if you are over 18 years of age and accept all the terms and conditions. Otherwise, it leaves the application and opts out of the terminal. Remember, if you record a joke and spread it with your friends, it is because you have applied for permission from the person who received the joke or gave it to you. You are solely responsible for this action."*

A button marked *"Continue*" is inserted immediately after this text.

A motion for a resolution was issued, proposing:

1. That the Director of the AEPD penalise MIRACLIA for an infringement of Articles 13 and 14 of the GDPR, which is defined in Article 83 (5) (b) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).

2. That the Director of the AEPD penalise MIRACLIA for an infringement of Article 6 of the GDPR, which is defined in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).

3. That the Director of the AEPD request MIRACLIA to comply, within a period to be determined, with the rules on the protection of personal data, the processing operations which it carries out, the information provided to its clients and the procedure by which they must give their consent to the collection and processing of their personal data, with the scope set out in Article XI of the motion for a decision. This should also be implemented in all the countries of the European Economic Area in which MIRACLIA operates through the Juasapp application.

Notified to MIRACLIA of the above-mentioned proposal for a decision, this Agency received a written submission requesting that the measures be closed on the

basis of the following considerations:

A. What MIRACLIA calls 'Technical facts':

MIRACLIA is a telecommunications company operating a service called "Juasapp", which is subject to regulation of "*number-based interpersonal electronic communications service"*.

In that regard, it points out that the Juasapp service is in a different technical and data-processing environment from that presented in previous actions of the Agency and the Ordinary Justice. In fact, the scenario of the service in force on the dates of the complaints is dependent on the version of the service that has been audited by a professional telecommunications engineer (please provide a copy of the corresponding report) from which the following conclusions are drawn or "Final Opinion":

*'1. The interpersonal electronic communications service based on 'Juasapp' numbering has the attributes and characteristics defined in Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC), enabling it to be classified as a number-based interpersonal electronic communications service as defined in Article 2 (5) and (6) thereof.*

*2. The regulatory framework applicable to electronic communications services makes a clear distinction between the production of content, which entails editorial responsibility, and the transmission of content, which does not imply any editorial responsibility (Article 2 (4) EECC and judgments of the Court of Justice (Fourth Chamber) of 5 June 2019 Y of 13 June 2019) of the Court of Justice of the EU (CJEU).*

*3. The user of the interpersonal electronic communications service based on 'Juasapp' numbering (the person initiating the transmission) unilaterally determines the recipient of the service, for whom there are no constraints requiring that he is a user of the Juasapp service but is a freely chosen recipient on the basis of the public numbering resources on whose data, publicly accessible and known to the user, he does not process any 'Juasapp'.*

*4. From the start of the number-based interpersonal electronic communications service, 'Juasapp' is limited to providing the physical means, of their own or of third parties, for the transmission of the signal between who initiates the transmission and the recipient of the signal chosen by the latter, in compliance with the quality, privacy, security and transparency requirements laid down in that directive.*

*5. Juasapp does not record the conversation. The recordings are made by the user who has contracted the Juasapp service in a private domain assigned exclusively to that user (in the cloud by allocating a private URL) who, as part of his right to participate in the edition of the recordings and accepting the terms of use of 'Juasapp', unilaterally decides to record them for their personal use.*

*6.'Juasapp' also does not retain data of the final recipient other than those which, as a minimum, enable him to comply with the provisions of the data retention rules and to provide the service to the user of the data. I.e. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of electronic*

*communications services, transposed in Spain by Law 25/2007.*

*7.'Juasapp' offers the possibility for persons or entities, who make use of networks with public numbering resources to be chosen as recipients of transmissions by 'Juasapp' users, to apply for inclusion on a 'black list' in order to inhibit the receipt of electronic communications via the Juasapp service.*

*8. In accordance with Recital 173 and Article 95 GDPR, which states that the GDPR shall not impose additional obligations on natural or legal persons in relation to processing in the framework of the provision of public electronic communications services in public communications networks in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC"(Directive on privacy and electronic communications).In this regard, account should be taken of recital 34 of Directive 2002/58/EC: 'It is necessary, with regard to the identification of the source line, to protect the right of the calling party to reserve the identification of the line from which the call is made and the right of the person called upon to refuse calls from unidentified lines.' It is therefore necessary to respect the right of the user who initiates the transmission (bromists) not to present his telephone number to the recipient, since, first, user and recipient make use of public telephone resources, the right of the calling user is to be protected by means of (bromists) the right not to present his telephone number in order to communicate it to the recipient, since, first, user and recipient make use of public numbering resources and the right of transmission to which the calling is made, and the right of the calling party to communicate the telephone number to the recipient, first user and recipient making use of the second line identification, and the right of transmission to which the call is made, and the right of the calling user not to present his telephone number to the recipient.*

B. Which MIRALCIA calls "Regulatory Framework":

(1) The considerations described in Article 95 GDPR should apply to the number-based interpersonal communications service ("Juasapp"*) ("This Regulation shall not impose additional processing obligations on natural or legal persons in the framework of the provision of public electronic communications services in public communications networks in the Union in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC")*.

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

a. these cases fall outside the scope of the GDPR on the basis of Recital 18 and Article 2 (2) (c) GDPR, as they concern data processing carried out by a natural person in the course of a purely personal or household activity.

b. the sole controller is the user of "Juasapp" and not MIRACLIA.The user carries out the processing directly because it is the person who freely makes the necessary edition for the act of the joke (edits the joke to be spent; enter the phone number of the person receiving the call and press the push-button; decides whether to generate the file with the recording of the joke and thus the URL of it, which is personal and known only to the user).Moreover, it is always the user himself who broadcasts the joke in his particular environment.
MIRACLIA intervenes only to provide the number-based interpersonal electronic

communications service, which has been contracted by the user of the service. On this basis, he proposes that the Agency approach the bromists with the same action as against MIRACLIA.

C. During first and foremost the process of joke, the app user and controller does not derive any economic benefit, so recital 18 GDPR and Article 2 (2) (c) above apply.

(3) Click 'examples' of other companies providing number-based interpersonal electronic communications services for which, according to MIRACLIA, the Spanish Data Protection Agency has not carried out any investigation or inspection for similar reasons, where the communications service provider is never responsible (user of a telephone operator calling a known person and insults occur in communication; or calling a public or private centre to warn of the existence of a bomb; a computer attack in which the virus uses communication networks and storage of digital information to infect others; use of an app for a meeting by videoconference between publicly numbered subscribers, which allows the administrator to make a recording of the app; The 'Burovoi*'* interpersonal electronic communications service (https: //www.burovoz.es/), which allows its users to record telephone conversations between a user of the service and another person, who is not a user of the '*Burovoi'* service, but has a telephone number in the public numbering system.The functioning of this service is exactly the same as "Juasapp" and not only is 100 % legal but its recordings have been and are fully valid when presenting them as evidence in legal proceedings in Spain.

(4) On the subject of recordings of telephone calls made by 'Juasapp' users, Judgment No 114/1984 of 29 November, delivered by the Second Chamber of the Constitutional Court, states that '*Who records a conversation of others, irrespective of any other consideration, to the right recognised in Article 18.3 of the Constitution; On the other hand, a person who recorded a conversation with another person does not, by virtue of that fact alone, engage in conduct contrary to the aforementioned constitutional provision.*'

(5) Article 20 of the Spanish Constitution provides for and protects the rights to: '*To the literary, artistic, scientific and technical production and creation'*, all of which are part of the right to freedom of expression enjoyed by all Spanish citizens in general and the user of 'Juasapp'.

(6) In its final considerations, it adds that compliance with the data retention obligation imposed by Law 25/2007 enabled the entity to effectively and within the time limits set by the GDPR the rights of access, rectification and deletion which have been requested by multiple recipients of the jokes, as well as by the State Security Forces and Corps in order to investigate possible crimes.

C. With regard to the complaints set out in the Background to this decision, it states the following:

1. The complaint made by complainant 1 should not have been admissible for the following reasons:

(a) The complainant refers to identity theft by a police.

(b) The complainant did not contact MIRACLIA to request the exercise of ARCOPOL rights.

(c) It is very likely that the complainant suffered a joke from another competing service and therefore asks the Agency to require the telecommunications operators to obtain from the telecommunications operators a statement of calls received on the number of the person receiving the call.

(d) On 30/10/2018, the complainant received a letter from MIRACLIA informing him that 'Juasapp' did not have in his catalogue any jokes similar to that described in the catalogue and asked him to provide the URL of that recording for cancellation, if it were outside the Juasapp service. The complainant did not provide this information, so it is understood that the exercise of rights was sufficiently lent.

(e) We note in the file that the complainant provides a record of Whatsapp. However, 'Juassap' never sends the contents of the jokes by Whatsapp, as they can only be heard in the user's own application. Furthermore, the files of the recordings of the jokes that users can download onto their device have a file name which is not the same as that provided as evidence. It can therefore be inferred that there may have been an amending act and the evidence should be invalidated at that time.

(f) The company is seeking to examine the possibility of bringing a criminal action against him for false complaint and damage to the company's honour.

(g) Therefore, and given that MIRACLIA has always agreed to remedy users' rights, it asks the Agency to close this case as it responded to the request for access to its data and considered that, with the information available, the joke did not start from a 'Juasapp' user.

2. MIRACLIA also considers that the complaint lodged by complainant 2 should also have been declared inadmissible on the following grounds:

(a) The acquainted person (s) fully knows the bromist (s) and should therefore have brought the action against them and not against MIRACLIA, which does not process the data of the person who receives the call of joke.

(b) It is false that the abropated person received a call at 3: 30 in the early morning, since none of the 'Juasapp' jokes can be held at those local times. Moreover, Juasapp, as a number-based interpersonal electronic communications service, never makes calls to any recipient once the joke has occurred, as this is something that can only be done by the user of the app.

(c) The complainant did not contact MIRACLIA requesting the exercise of ARCOPOL rights.

(d) It is also false that once the right of access 'Juasapp' has been exercised it continues to send emails. Juasapp has never committed or commits such practices.

D. As regards the facts established, MIRACLIA makes the following observations:

.Done at 1: MIRACLIA owns a number-based interpersonal electronic communications service accessed by means of an application called 'Juasapp'.There is a website with the same name, 'Juasapp', as a commercial and user information service that is not part of the electronic communications service provided by MIRACLIA and has not been the subject of a complaint.

.Done at 2: Under Article 95 GDPR, interpersonal electronic communications services based on public numbering resources are not required to identify the call operator or platform owner or to indicate where to obtain information on the call or on the

exercise of rights. As mentioned above, 'Juasapp' is an application providing access to an interpersonal electronic communications service, the user of which reserves the right or not to identify and personally record that call.

.Done at 4: The reference to the hosting of the jokes on a public site is wrong. Audio access is provided via a token based URL as used on thousands of privately accessible websites (e.g. the parcel tracking website of a messaging service or a multitude of public services for the payment of fines).The URL referred to by the inspector is automatically generated on the server, which means that, as it is not a fixed or static URL, it can only be accessed by the user of the interpersonal electronic communications service based on public resources whose name is 'Juassap'.Only the sender of the joke and the recipient of the joke have access to that URL if the sender of the joke wishes to do so (it is their responsibility).

.Done at 5: this proven fact indicates that the link http: //juasapp.mobi/web/change allows you to change the country where the app operates. However, it is not known how the Agency has accessed this pre-production platform which is a prototype of evidence that has never worked in production and therefore could never be used by an end-user as an electronic communications system. The purpose of that prototype was to offer the electronic communications service in multi-platform mode, such as Skype, which can be used on an app or on a computer independently of its Operating System.

.Done at 9: In any catalogue of MIRACLIA's jokes no jokes appear to replace any body or person, let alone the police. As well as copying the catalogue of MIRACLIA, there are a multitude of other fungi services, but they are likely to have introduced some of them as a substitute for the police, but MIRACLIA is not aware of this.

E. In response to the considerations set out in ground IV of law concerning the definition of processing of personal or domestic data, MIRACLIA makes the following statements:

.Personal or domestic conversation takes place through the provision of a number-based interpersonal electronic communications service. Numbering data are public resources that are not processed by an operator. The user of that service and which is processed is who enters the service and chooses the recipient of the call on the basis of those public resources. It is that user who recorded the call using tools complementary to the basic electronic communications service. The cited references of the CJEU do not refer to the case of such services.
Furthermore, it is the user who decides freely and freely to whom he steers the joke within his known contacts or family or friends.

.The judgment of the Court of Justice in Case 10/07/2018, according to which '*an activity shall not be regarded as exclusively personal or household where its purpose is to give an indeterminate number of persons access to personal data or where the activity extends, even in part, to the public space and is therefore directed outside the private sphere of the person processing the data, is not valid for Juasapp*'.The purpose of the service is to establish an electronic communication initiated by the bromist, who decides to record it and to have access to its private recording. Sharing it in his private circle is a decision of the bromist, who in the Tyc is told that he may infringe regulatory standards depending on the processing of that data (his own private data).The purpose of the service is under no circumstances to share the recording indiscriminately.

.The proposal states that "MIRACLIA's*action is essential since without it it would not be possible to process data as it is done in the process. MIRACLIA provides the means of making the call, providing the means of choosing a joke, and providing the means to record and store a joke.*"In this regard, MIRACLIA states that it is logical that it should be in this way, since it has defined Juasapp as a number-based interpersonal electronic communications service with that functionality and should be governed in its entirety as described by the regulatory standards in force (Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC), as defined in Article 2 (5) and (6) thereof.

F. The constitutional principle itself

*'This principle of "personal responsibility" has been referred to, which means that a person can only be held responsible for his own facts, that is to say, not for one thing or an animal.'*
(source: https: //www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2009-10021100252_ANUARIO_DE_DERECHO, Antonio Cuerda Riezu)

In accordance with this principle and in greater detail in the present case, we can demonstrate that Juasapp' as a number-based interpersonal electronic communications service cannot bear any responsibility for the act undertaken by the user of 'Juasapp', just as a gun manufacturer can never be held liable for the act committed by a person misusing that gun.

G. Other final considerations

.The URLs that may be received by the person who receives the call of joke from the bromists, once the call has been recorded, are NOT public URLs. The URLs generated by the server software for the Juasapp user are private and cannot be indexed by search engine Spiders such as Google, Bing or Yahoo.

.That the Agency take into account File No: TD/00007/2017, in which the case concerns a person who has been acquitted by the radio 4G broadcaster and the live broadcast and the entire audience of radio 4G and which ends up in the proceedings.

.All the points made in this letter are confirmed both in the technical audit which is now in the process of being endorsed by COIT (Colegio Oficial de Ingenieros de Telecomunicaciones) and in the conditions of use accepted by the user before being able to use the platform.

Finally, he asked for a hearing in person in order to clarify before the Agency's investigators/inspectors the points raised and warned that, if their interests were not met, he reserves the right to go to other higher or judicial bodies in Spain and Europe.

Withyour written observations, you provide a copy of the report on the technical audit in question, which was carried out by a telecommunications engineer on 29/07/2020. This report is structured in four sections:

*.Objectives and methodology of the work.*
*.Description of the Juasapp service.*
*.The audit findings*

*.Final opinion.*

According to the petitioner, it is based on face-to-face interviews, practical 'Juasapp' execution tests on two mobile devices and the testing of messaging, recording and metadata tools, although it does not provide details on the development of these tests, merely listing a number of findings.

The following is stated in the section "Audit Results":

*'As regards the specific analysis of the Juasapp service, we found the following facts:*

*(a) Only a given user registered with the Juasapp service can start the conversation.*

*(b) The user of the Juasapp service is the only party to the proceedings who can freely determine the addressee of the conversation*

*(c) Public numbering resources are used to determine the addressee of the conversation.*

*(d) It is not required, or verified or verified by any means, that the recipient of the conversation is a user of the Juasapp service.*

*(e) Once the connection between the user of Juasapp and the recipient of the conversation has been established, the direct exchange of interpersonal information via electronic communications networks between the two persons is permitted.*

*(f) 'Juasapp' offers the user contracting that service a set of pre-configured templates for the editing of a voice message.*

*(g) The user contracting the Juasapp service is who freely chooses between them to determine the content of the message to be transmitted.*

*(h) The recording is made on a personal and private domain assigned exclusively to the user of the 'Juasapp' service, as a service that provides 'Juasapp' to the cloud user on his own premises.*

*(I) The recording domain offered by 'Juasapp' to the user of that service is a private and secure domain.*

*(j) The final decision as to whether or not to record the message in his private domain lies exclusively with the user of the 'Juasapp' service.*

*(K) 'Juasapp' offers the user contracting that service an interactive metadata toolkit to perform on possible actions on the edited message.*

*(L) 'Juasapp' offers any person or entity that is part of a plan for the use of public numbering resources the possibility to join 'blacklists' so as not to receive more calls from Juasapp users.*

*(m) In fact, certain numbers in the public numbering plan are by default included in that 'black list' (091, 061, 112, 092, etc.).*

*(N) 'Juasapp' provides the physical means, either of its own or of a third party, for the transmission of the signal between who initiates the transmission and the recipient of the transmission chosen by him.*

*(o) 'Juasapp' does not retain data of the final recipient except those which, as a minimum, enable him to comply with the provisions of the legislation on data retention*'.

In the previous section, the 'Description of the Juasapp service' label describes the information provided by MIRACLIA to the auditing engineer, which corresponds literally to the 'facts' detailed as a result of the audit.

That report includes an Annex II relating to the 'starting points and reference rules'.This Annex refers to the definition of an interpersonal electronic communication service introduced by the European Electronic Communications Code (EECC), which is those that pertain to the exchange of interpersonal and interactive information via electronic communications networks between a finite number of persons, in which the recipients are identified by the persons initiating or participating in the communication, and adds the following:

*'In the conditions of use of the JUASAPP application it is stated in Article 6 that 'like any telecommunications service, the use of JUASAPP services for the purpose of harming or harming nobody is illegal'.There is therefore a contractual declaration that JUASAPP is a service subject to telecommunications regulation and therefore an implicit acknowledgement that it is an electronic communications service in such a case.'*

As PROBED to this Resolution, we consider that:

1. MIRACLIA owns the mobile application and web service called 'Juasapp'.This app allows users to make telephone jokes to third parties. The user selects a joke and a 'victim', who is contacted by MIRACLIA by telephone from his own system by means of a hidden number (joke call), with a recording of the conversation made available to the user of the app.

Theuse of the above mobile app and web services is regulated in the document entitled 'Terms and Conditions of Use of the Service', which is stated to be reproduced in this document for purposes of proof. The following can be highlighted from the content of this document:

*< < When using the Service, you will be bound by the Terms of Use and Privacy Policy, expressly accepting its fulfilment and by entering into force a legally binding contract with us... if you do not agree with these Terms of Use or Privacy Policy, we recommend you to disinstall the application of your terminal.*

*3. Definition of the service*

*JUASAPP is an application that allows the user to send jokes consisting of an audio file pre-recorded by telephone to the destination selected by the user. The user may select from a list of jokes and indicate both the destination line and the time at which he wishes the recipient to receive the joke. Once the joke has been made, the app has the functionality of sharing and recording the audio file (hereafter "recording"). however, it will be essential for the user to have the explicit consent of the person who received the joke in order to be able to obtain it and subsequently make use of it.*

*(...)*

*NOTE: Since the personal data of the recipient of the call are stored solely and exclusively at the terminal of the user of the application (customer), in the event that the user removes the application at his terminal or deletes the data associated with it at its terminal, the latter may cease to function in the sense that the deleted information disappears from it.*

*(...)*

*5. Payment services*

*The use of the app may entail a cost...*

Theamounts purchased will expire after 6 months without the use of the application. At that time, the user's content may be deleted.

*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 telephone pins to a recipient and then reproduce, download or share the joke. With the acceptance of these Terms and Conditions of Use of the Service, the Juasapp User assumes the following responsibilities:*

*(...)*

*(b) Different and record sweets*

*The User, as owner of the recording, is fully responsible for obtaining the explicit and unambiguous consent of the person who received the joke, for the recording and dissemination of it.*

*The laws allow the recording of any telephone conversation subject to the consent of at least one of the parties involved in the conversation. A user will not be able to download a recording without obtaining the prior consent of the recipient of the recording.The operation of the Service prevents the creation of grabbing if the user of JUASAPP does not expressly accept such a precondition.*

In*order to share jokes publicly, the Service requires that the person sharing the joke has obtained permission to do so from all the participants in the call. MIRACLIA is not liable for the consequences of failure to obtain the consents necessary to share the Grabbing, and it is obliged to compensate third parties or MIRACLIA for any claims arising out of its actions.*

*(...)*

*8. Limitation of responsibilities*

*Responsibilities of MIRACLIA:*

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

*MIRACLIA never decides on the purpose, content and use of the processing of the recording and therefore cannot be held responsible for it.*

*(...)*

*If the recipient of the joke (as data holder and exercising his right of objection or cancellation) or the sender of the joke (as owner of the recording) requests MIRACLIA to cancel the recording, the recording is automatically removed fromthe servers serving MIRACLIA.*

*However, prior to the exercise of the right of objection or cancellation by the recipient, the joke could be downloaded from the User's device, the recording being outside the reach of the MIRACLIA and, therefore, the entity is not responsible for the use, disclosure and modification of it by the User.*

*(...)*

*9. Protection of data*

*We have set up a Privacy Policy to explain how we collect and use information about you (the user)... > >.*

2. The Agency's inspection services, on 6, 9 and 12 September 2019, carried out tests consisting of downloading the app into a mobile terminal and making use of it by making calls for jokes. As a result of these actions, the following findings were made:

.During the installation process the user receives, inter alia, the following messages:

*'Please read these Legal Terms and Conditions in detail and please accept if you are over 18 years of age and accept all the terms and conditions. Otherwise, it leaves the application and opts out of the terminal. Remember, if you record a joke and spread it with your friends, it is because you have applied for permission from the person who has received the joke and has given it to you. You are solely responsible for this action."*

*'Miraclia does not collect data from the recipients of the jokes. Miraclia's activity is to provide a means of telecommunications to enable the owner of the telephone downloading the app to choose a joke and to record it, with data relating to the recipient of the call stored on the user's own terminal without Miraclia retaining information on the recipient's telephone number. Miraclia provides a cloud storage service for the customer's audio files and at no time does it disseminate or share that information with anyone, since it is private information of the user of the application" (this paragraph is also included in the privacy policy).*

A button marked "Continue" is inserted immediately after these texts.

.The Juasapp application consists of 3 tabs: 'Listed', 'Examples' and 'My bromas'.In this last tab, the jokes made by the bromist will be saved if they are not removed.

.The telephone number of the incoming joke call appears as 'Private number' in all cases.

.In the test installed version, the latest one available in the Android 'Play Store' application shop, the bromist, has no choice as to whether or not the joke is recorded. the joke is always recorded, unless the recipient decides to delete it in accordance with any of the procedures laid down for that purpose. If this is not the case, the recording remains in the MIRACLIA systems until the bromist decides to remove it or, as a general rule, for a period of 6 months after the use of the application, established by the entity itself.

.At no time during the telephone conversation identifies the Juasapp application as the call manager or the developer MIRACLIA as owner of the platform. Therefore, the recipient of the joke does not know where to contact in order to obtain more information about the call or to exercise his rights.

.At no time is the bromist named.

.Nor is it reported at any time, during the course of the joke, that the conversation is being or may be recorded.

.At the end of the joke, the following phrase is heard: "A friend of his own has spent a joke. If you do not want your friend to listen, download or spread the joke, or if you do not want to receive more jokes, click 5 with your keyboard after the signal. Beeep'

From the end of the joke until the word occurs, a period of silence of 10 seconds

elapses.

.The “erasing” of the record of the joke and the inability to continue to receive jokes by pressing key 5 after hearing the signal indicated in the final phrase has been unstable in the tests carried out. On one occasion when key 5 is pushed before the signal and on another occasion the mechanism failed; on two other occasions, it was only clicked once after the signal and was successfully removed. It was found that there is no confirmation of erasing of the joke, simply when approximately 10 seconds after the indicated signal to press key 5, the communication is cut off.

In cases wherethe removal worked correctly, the joke disappears from the list of jokes made by the bromist and cannot therefore be shared, downloaded or listened to. It has also been found that the telephone number was blocked to receive more jokes.

.There are three icons on the list of jokes made by the bromist, next to each of the jokes not removed by the joke receiver in accordance with the procedure indicated: one to download the audio file of the recording of the telephone conversation of the joke, one to listen and a third to share it. In the latter case, the link to the audio file of the recording is sent via the media chosen to share it. This is the only moment when the link to the audio file is known to the bromist.

.In the event that the bromist leaves the finger pressed on a certain joke in the list of jokes made, a pop-up window appears offering the possibility of removing the audio file from MIRACLIA systems, but this action is not as intuitive as the three above, without a specific icon.

.On the saved jokes, there is the telephone number of the destination, type of joke, date and time of making.

.Uninstalled the app and re-installed, it can be seen that the telephone numbers of the jokes made appear as ‘??????????’, which suggests that this data is stored locally and not on the servers of MIRACLIA.

.Joke calls may be instantaneous or programmed by specifying the date and time of execution. In this case, the recipient’s telephone is stored in MIRACLIA’s systems until the call is made. In that regard, MIRACLIA has stated in its submissions that the telephone number to which the joke is addressed is linked to the call to be made, which disappears from its systems when the call is made.

Theacting inspector programmed a joke at his terminal for delayed execution and the terminal was subsequently switched off. The call was made at the scheduled time, meaning that the phone was stored in the MIRACLIA systems until the time of performing the joke (minutes, hours, days or months).

.There are only two options for deleting the recording: the bromist follows the erasure procedure described since the application; or to ask MIRACLIA, a question which is difficult for the person concerned, considering that it is not apparent at any time who handles the call or the undertaking responsible for the call. Furthermore, to do so, the person concerned will need to know the link to the audio file and do not have this information, unless it is provided by the user (the joke can be removed by knowing the

url of the recording and using the mechanism provided on the web next to the request to block the telephone line number).

3. MIRACLIA offers on its website 'juasapp.es' a free and immediate system to include a telephone number in the list of blocked telephones.

The inspection carried out a test by registering in that system the telephone number corresponding to the second SIM of the inspector's terminal. Subsequently, an attempt was made to make a joke to that telephone number and the application did not allow it to be executed.

4. MIRACLIA does not have a platform on which the gumps made are published so that any third party can access them, but the recordings of the jokes are hosted on a public site, which makes it possible to access them via the link to the audio file, which can be disseminated indiscriminately by the bromist user.

5. On 02/12/19 it was verified that using the link http: //juasapp.mobi/web/change the country in which the app operates can be changed. These countries include both the European Union (Austria, Belgium, Germany, etc.) and outside the European Union (China, the United States, Argentina, Brazil, South Korea, etc.).It is also verified that the terms and conditions of use of the service are written in English, Italian, French and German.

6. On 03/12/2019, the application was installed, verifying that the process does not provide an option to shape another country or another language, although the terms and conditions of use of the service are written in Spanish, Italian, French and German, the same languages as are available when accessing the website on the Internet.

7. The complainant 1 has stated that on 01/09/2018 he received on his mobile telephone line 639610479 a joke call via the 'Juasapp' app, in which a person wanted to be a police officer. Denounces that the call was recorded and disseminated to third parties without their knowledge or consent; and that the call is made from a hidden number.

8. Complainant 2 has stated that, on 29/06/2019, she was the subject of a telephone call for jokes made using the 'Juasapp' application, which was recorded and broadcast on social media with a reference to her name without her permission (he provides the link to the audio which is the subject of the complaint 'http: //juasapp.mobi: 8080/...').

On 26/08/2019, the inspection services accessed the 'juasapp.es' website, the URL corresponding to the recording of the joke made to complainant 2. It is checked that using the right-hand button different options are displayed, including reproducing and downloading the recording.

9. The Agency's inspection services have found that the jokes reported by complainants 1 and 2 appear in the catalogue of broths available in 'Juasapp'.

**Concerned Supervisory Authorities**
The following supervisory authorities have been informed of this final decision:

- SA Belgium
- Berlin SA
- Cyprus SA
- SA Denmark
- SA France
- SA Greece
- SA Hungary
- SA Ireland
- SA Lower Saxony
- SA Norway
- SA Poland
- SA Saxony
- SA Slovakia
- SA Sweden
- Mecklenburg-VorpommernSA.

**NORM allegedly infringed**
The complaint concerns the failure of MIRACLIA to compile with the request of those who suffer from the brown regarding the following Articles of the GDPR:

- Legality of the processing (Article 6)
- Transparency and Information (Articles 12, 13 and 14)

**Final decision on action to be taken**

The legal basis of the proposed Resolution is as follows:

Theseproceedings are initiated on the basis of complaints received at this Agency against MIRACLIA, in which the persons concerned (the person who receives the call for jokes) complain about the use of their personal data to make a joke, using the 'Juasapp' application, by calling their mobile telephone lines by telephone. The recording of the call without the knowledge of the persons concerned and the dissemination of that recording to third parties, including without their consent, are denounced.

The procedure is therefore aimed at an overall analysis of the Juasapp application from the point of view of the rules on the protection of personal data and in relation to persons who receive calls of jokes.

Any analysis of the position of the users of the application (bromists), as well as of the information MIRACLIA provides to them and of the processing of their personal data, is omitted.

On the basis ofthe above, any conclusions drawn from the present proceedings will not lead to a ruling on the above aspects that have been discarded.

IV

As a preliminary point, it is necessary to consider the argument put forward by MIRACLIA in relation to its position in the personal relationship between a bromist and a person called a joke. It considers that its intervention is limited to providing a leisure environment between private individuals, who acts as an intermediary in a relationship between private individuals.

In accordance with this approach, MIRACLIA takes the view that the rules on the protection of personal data are not applicable to the present case, since spending a joke through an application or a means in which the user is sovereign of the information provided is an act carried out at the domestic or personal level and thus excluded from the scope of protection of that legislation in accordance with Article 2 (2) GDPR and Article 2 (2) (a) of the LOPDGDD.Article 2 (2) GDPR reads as follows:

'*2. This Regulation does not apply to the processing of personal data:*
*(c) carried out by a natural person in the course of a purely personal or household activity'.*

The Agency, on the other hand, considers that the action of the requested entity cannot be included in this exception for three reasons:

.MIRACLIA is not a natural person: Article 2 (2) (c) GDPR, by providing for the exception indicated, explicitly refers to the processing of personal data by a natural person.
.Its activity is carried out in connection with a professional or commercial activity. It is set up as a limited company with a view to making a profit and having a commercial character.
.The GDPR applies in full to controllers or processors who provide the means to process personal data related to personal or household activities (if actually).

On these issues, recital (18) GDPR states:

*"This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors who provide the means to process personal data related to such personal or household activities."*

We are dealing with business activities, with a business model based on the realisation of jokes through an application in exchange for a price.

In order to define what is to be regarded as treatment of a purely personal or domestic nature, although the application of those provisions may be ruled out in this case without it being necessary to go into that analysis, account should be taken of the case-law of the Court of Justice in Lindqvist, Rynes and Witnesses of Jehová (judgment of 10 July 2018, C-25/17).

According to these judgments, it can be considered that the CJEU generally understands that the exception of activities of a purely personal or domestic nature must be interpreted strictly, only where the processing of data affects 'incidentally' the private life or privacy of 'other persons', other than the controller processing the personal data. The Court also states that the nature of personal or household activities is not defined exclusively as opposed to the dissemination of the data, as MIRACLIA seems to suggest, but that such dissemination implies that the processing of personal data relating to the private or family life of individuals cannot be considered to be excluded from the protective legislation, so that there may be other cases in which, even when personal or household personal data are concerned, it cannot be regarded as falling within the exception provided for in Article 2 (2) (c) of the GDPR.

It is important not to lose sight of the processing of personal data carried out in the present case: it consists of a telephone call, to a telephone of a third person, whose voice, when replying to the call, is recorded in MIRACLIA's technical system. As can be seen, in this case the private life or privacy of others is not 'incidentally' affected, but the very purpose of that data processing is precisely the voice of the third person called. In other words, the processing of the personal data of the third party named is not a mere 'incidental' inconvenience within a more general data processing, but the use of his personal data is precisely the purpose of the processing. Consequently, such data processing of the voice of the person receiving the call cannot in any event be regarded as merely incidental, but as a 'principal' processing.

The Court of Justice of 10 July 2018, C-25/17, Jehová's Witnesses, sets out an interpretation of the concept of purely personal or household activities and reads as follows:

*42 As the Court has held, the second indent of Article 3(2) of Directive 95/46 must be interpreted as covering only activities which form part of the private or family life of individuals. In that regard, an activity cannot be regarded as exclusively personal or household within the meaning of that provision where it is intended to allow an indefinite number of persons access to personal data or where 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, to that effect, judgments of 6 November 2003, Lindqvist, C-101/01, EU: C: 2003: 596, paragraph 47; Of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU: C: 2008: 727, paragraph 44, and of 11 December 2014, Ryneš, C 212/13-, EU: C: 2014: 2428, paragraphs 31 and 33).*

In the case of MIRACLIA, it appears that the 'abropated' natural persons transfer information to MIRACLIA, since the voice of the person receiving the call is recorded in the application provided, and also those who are to be bromists also transmit it to MIRACLIA, because they provide MIRACLIA with the telephone numbers for the calls to be made by MIRACLIA.This telephone is registered in the organisation's systems until the call is made, the conversation is recorded for the purpose of providing a multimedia content service accessed via mobile devices, offering the possibility to reproduce, download and share the audio file. This means, first of all, that this activity is directed outside the personal and private sphere of the bromist, as interpreted by the CJEU, which in any event excludes it from the 'exclusively personal and private' exception.

Itfollows that 'bromists' natural persons would transmit personal data to

MIRACLIA, which registers (that is to say, 'processes' those data) by recording them. However, MIRACLIA also 'treats' in its systems the telephone number of those third parties, potentially (if not materially) establishing a link between a certain telephone number and a certain voice recorded in its systems. In other words, MIRACLIA processes personal data to which the exception referred to above cannot in any event apply.

In addition, although there is initially no link between MIRACLIA and the 'victim', data processing is also carried out in the form of a register of those who do not wish to receive more jokes.

MIRACLIA's action is essential since, without its tender, it would not be possible to process data. MIRACLIA provides the means of calling, providing the means to choose a joke, and provides the means to record and store a joke, which means that it determines the means of processing and the purposes, organises, encourages and coordinates the activities of bromists through its Juasapp application, and is therefore involved, together with the bromists, in determining the purpose and means of processing the personal data of the person called. Moreover, MIRACLIA, 'having regard to its own (commercial) objectives', influences and encourages bromists, and must therefore be held responsible, together with the bromists, for the processing of data carried out by those who have been acquitted.

V

Another preliminary issue raised by MIRACLIA relates to the existence or otherwise of personal data. He questions whether the information can be regarded as personal data, since MIRACLIA is unable to identify the person who receives the call of jokes in a simple manner and without disproportionate means, and points out that the only person who can identify the person who receives the call is the user, who is anonymous to the entity.

It adds that it is not able to identify the person who receives the call of joke or to link him with any other data and that voice is not personal data if it does not allow the holder to be identified or if disproportionate efforts are necessary to identify him.

The GDPR defines the concept of 'personal data' in Article 4.1) as: "any information relating to an identified or identifiable natural person ("the data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

According to those definitions, information on the persons to whom the jokes are made using the 'Juasapp' application collected by MIRACLIA complies with the definition of personal data. In addition to the telephone number, MIRACLIA also records the voice of the abropated persons through the appropriate recording of the joke, which is likely to be broadcast, as well as other user data.

In relation to voice recording, Report 497/2007 of the Legal Office of the Agency states that "sound recordings shall enable a person to be identified, even more so this

recording is attached to a file and will therefore fall within the scope of the LOPD".In the same vein, the Audiencia Nacional (National High Court) has expressed its view.

To the latter, I would add that the judgment of the Audiencia Nacional (National High Court) of 19/03/2014 (rec.176/2012) states that 'the voice of a person constitutes personal data, as is clear from the definition given therein in Article 3 (a) of the LOPD, such as < any information concerning natural persons identified or identifiable > >, which is not disputed'.

This is a broad concept which may include objective information, such as first name and surname, or subjective information, such as the assessment of an examiner in a professional examination. This has been understood by the CJEU, for example, in the CJEU judgment of 20 December 2017, C-434/16, Peter Nowak.

That the GDPR regards voice as personal data is undeniable. Opinion 4/2007 of 20 June 2007 of the Art. 29 Working Party on the concept of personal data (WP136) also contains examples. In example 2 on Telephone banking, it states: 'In telephone banking operations, where the voice of the customer instructing the bank is recorded on a tape, the instructions recorded must be regarded as personal data'.Similarly, both this Opinion 4/2007 and Opinion 3/2012 on the evolution of biometric technologies (WP193) state that voice can be both personal data, raw and also used with biometric techniques.

In order for that acoustic characteristic of the human person to be considered personal data, the GDPR determines that that information must relate to an identified or identifiable natural person and considers that person who can be identified, directly or indirectly through that personal data, as an identifiable person.

MIRACLIA is based on a false premiss that this is not personal data because the MIRACLIA entity itself could not identify the person whose voice is recorded (that is to say, the 'data subject', the person who receives the call), since it does not store the addressee's number.

This argument is misguided. The data protection rules (recital 26 of the GDPR) are based on a comprehensive protection of the fundamental right to data protection of a natural person. therefore, as we have explained above, the exceptions must be interpreted strictly and the concept of personal data must be interpreted broadly.

Recital 26 of the GDPR, in the part of which is now relevant, reads as follows:

*"The principles of data protection should apply to all information relating to an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. In determining whether a natural person is identifiable, account should be taken of all the means, such as uniqueness, reasonably likely to be used by the controller or by any other person to identify the natural person directly or indirectly".*

As can be seen, the GDPR considers that a person is identifiable when that person can be identified either by (i) the controller or by (ii) any other person.

As we haveseen above, the 'bromist' could be regarded as the controller together with MIRACLIA, so that, in those circumstances, there is no doubt that the bromist can identify the voice of the person who is the recipient of the call. However, even if it were considered that the bromist is not a controller, it would be regarded as a 'third person other than the controller', and the GDPR considers, even in that case, that the 'person called a joke' is a person identifiable by the 'bromist', which determines that the data of that identifiable person's voice must be regarded as personal data.

The data protection rules, therefore, do not restrict the concept of 'personal data' or 'identifiable person' solely to cases where the controller is able to identify, directly or indirectly, the data subject whose data are being processed (the person who receives the call), but extends the scope of the protection beyond that circumstance, and considers that if that person (the person receiving the call) considers that, as a result of the means made available to him or her by the broker, that person is not directly responsible, he or she considers that if that person (the person who receives the call) is directly responsible, as a result of the means made available to the broker by the data controller, who is not a person who is directly responsible, and considers that if that person (the person who receives the call), as a result of the means made available to the broker by the data controller, is not directly responsible.

In the event that two joint controllers are considered to exist in respect of the same processing, the CJEU has dealt with the fact that data protection law does not require or imply that each of them has access to the personal data in question, so that there may be one of those controllers who, without having access to the personal data, will remain responsible (see paragraph 69 of the judgment of 29 July 2019, C-40/17, Fashion ID, which in turn cites paragraph 29 of the judgment of 5 June 2018, C-210/16, Wirtschaflesvá of 10 July 2018, paragraph 65 of the judgment of, C-25/17, Fashion ID, which in turn cites paragraph of the judgment of, WirtschaflesBA, paragraph of the judgment of, Case, Fashion ID.

VI

Article 5 'Principles relating to processing' of the GDPR provides:

*'1. personal data shall be:*

(*a) processed lawfully, fairly and transparently in relation to the data subject ('lawfulness, loyalty and transparency');*

*(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

(*c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

(*d) accurate and, if necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

(*e) maintained in such a way as to allow the identification of data subjects for no longer than is necessary for the purposes of the processing of personal data; personal*

*data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

*(f) processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by the application of appropriate technical or organisational measures ('integrity and confidentiality').*

*2. The controller shall be responsible for and able to demonstrate compliance with paragraph 1 ('accountability')'.*

In relation to the above principles, account is taken of Recital 39 of the GDPR:

*'39. Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that personal data are not stored longer than necessary, the controller should set deadlines for their erasure or periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a way that ensures adequate security and confidentiality of the personal data, including to prevent unauthorised access to or use of such data and of the equipment used for the processing."*

VII

Article 4 of the GDPR, entitled 'Definitions', provides:

*"(2) "treatment": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,*

*consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.*

According to those definitions, the use by that entity of the information (personal data) which it collects from the acquitted person constitutes the processing of personal data, in respect of which the controller must comply with the principles laid down in Article 5 (1) GDPR, according to which personal data shall be 'processed in a lawful, fair and transparent manner in relation to the data subject (lawfulness, loyalty and transparency)'; and developed in Chapter III, Section 1, of the same Regulation (Article 12 et seq.).

Article 12 (1) of that Regulation requires the controller to take appropriate measures to 'provide the data subject with any information referred to in Articles 13 and 14 and any communication pursuant to Articles 15 to 22 and 34 relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular any information addressed to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. At the request of the data subject, the information may be provided orally provided that the identity of the data subject is demonstrated by other means."

Article 13 of that legislation specifies the 'information to be provided where personal data are obtained from the data subject' and Article 14 of that regulation refers to 'information to be provided where the personal data have not been obtained from the data subject'.

In the first case, where personal data are collected directly from the data subject, the information shall be provided at the same time as the data collection takes place. Article 13 GDPR details this information in the following terms:

*'1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*

*(a) the identity and contact details of the controller and, where applicable, of his or her representative;*

*(b) the contact details of the data protection officer, if any;*

*(c) the purposes of the processing for which the personal data are intended and the legal basis for the processing;*

*(d) where the processing is based on Article 6(1)(f), the legitimate interests of the controller or of a third party;*

*(e) the recipients or categories of recipients of the personal data, if any;*

*(f) where applicable, the intention of the controller to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or, in the case of transfers referred to in Articles 46 or 47 or the second subparagraph of Article 49(1), reference to the appropriate or appropriate safeguards and the means to obtain a copy thereof or to the fact that they have been provided.*

*2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:*

*(a) the period for which the personal data will be stored or, where that is not*

*possible, the criteria used to determine this period;*

*(b) the existence of the right to request from the controller access to and rectification or erasure of personal data concerning the data subject, or restriction of processing, or to object to processing, as well as the right to data portability;*

*(c) where the processing is based on Article 6(1)(a) or Article 9(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal;*

*(d) the right to lodge a complaint with a supervisory authority;*

*(e) whether the provision of personal data is a legal or contractual requirement, or a necessary requirement for entering into a contract, and whether the data subject is obliged to provide the personal data and is informed of the possible consequences of failure to provide such data;*

*(f) the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) and, at least in such cases, meaningful information on the logic involved as well as the significance and expected consequences of such processing for the data subject.*

*3. Where the controller plans to further process personal data for a purpose other than that for which they were collected, it shall provide the data subject, prior to such further processing, with information on that other purpose and any relevant additional information as referred to in paragraph 2.*

*4. The provisions of paragraphs 1, 2 and 3 shall not apply where and to the extent that the information is already available to the data subject.'*

In the second case, where the personal data are not obtained from the data subject, the information to be provided to the data subject is set out in Article 14 GDPR:

*'1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:*

*(a) the identity and contact details of the controller and, where applicable, of his or her representative;*

*(b) the contact details of the data protection officer, if any;*

*(c) the purposes of the processing for which the personal data are intended and the legal basis for the processing;*

*(d) the categories of personal data concerned;*

*(e) the recipients or categories of recipients of the personal data, if any;*

*(f) where applicable, the controller's intention to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or, in the case of transfers referred to in Articles 46 or 47 or the second subparagraph of Article 49(1), reference to appropriate or appropriate safeguards and the means to obtain a copy thereof or to the fact that they have been provided.*

*2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:*

*(a) the period for which the personal data will be stored or, where that is not possible, the criteria used to determine this period;*

*(b) where the processing is based on Article 6(1)(f), the legitimate interests of the*

*controller or of a third party;*

*(c) the existence of the right to request from the controller access to and rectification or erasure of personal data concerning the data subject, or restriction of processing, and to object to the processing, as well as the right to data portability;*

*(d) where the processing is based on Article 6(1)(a) or Article 9(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal;*

*(e) the right to lodge a complaint with a supervisory authority;*

*(f) the source from which the personal data originate and, where applicable, whether they come from publicly available sources;*

*(g) the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) and, at least in such cases, meaningful information on the logic involved as well as the significance and expected consequences of such processing for the data subject.*

*3. The controller shall provide the information referred to in paragraphs 1 and 2:*

*(a) within a reasonable time after the personal data have been obtained, and at the latest within one month, taking into account the specific circumstances in which the personal data are processed;*

*(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or*

*(c) if it is intended to be disclosed to another recipient, at the latest at the time the personal data are first disclosed.*

*4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.*

*5. Paragraphs 1 to 4 shall not apply where and insofar as:*

*(a) the data subject already has the information;*

*(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or to the extent that the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of such processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;*

*(c) obtaining or disclosure is expressly provided for by Union or Member State law to which the controller is subject and which provides for appropriate measures to protect the data subject's legitimate interests; or*

*(d) where personal data must remain confidential on the basis of an obligation of professional secrecy governed by Union or Member State law, including an obligation of secrecy of a statutory nature'.*

Article 11 (1) and (2) of the LOPDGDD provides:

*'Article 11. Transparency and information to the data subject*

*1. Where personal data are obtained from the data subject, the controller may*

*comply with the information obligation laid down in Article 13 of Regulation (EU) 2016/679 by providing the data subject with the basic information referred to in the following paragraph and by indicating an electronic address or other means allowing easy and immediate access to the remaining information.*

*2. The basic information referred to in the previous paragraph shall contain at least:*

*(a) the identity of the controller and his representative, if any;*

*(b) the purpose of the processing.*

*(c) the possibility of exercising the rights set out in Articles 15 to 22 of Regulation (EU) 2016/679.*

*If the data obtained from the data subject are to be processed for profiling, the basic information shall also include this circumstance. In such a case, the data subject shall be informed of his or her right to object to the adoption of automated individual decisions which produce legal effects on him or similarly significantly affect him or her, where this right exists in accordance with Article 22 of Regulation (EU) 2016/679.'*

In relation to this principle of transparency, account is also taken of recitals 32, 39 (already mentioned), 42, 47, 58, 60 and 61 of the GDPR.Part of the content of these recitals is reproduced below:

*(32) Consent must be given by a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject's wishes to consent to the processing of personal data relating to him or her...*

*(42)... In order for consent to be informed, the data subject must be aware of at least the identity of the controller and the purposes of the processing for which the personal data are intended...*

*(47) The legitimate interests of a controller, including that of a controller to which personal data may be disclosed, or of a third party, may constitute a legal basis for the processing, provided that the interests or the rights and freedoms of the data subject are not overridden, taking into account the reasonable expectations of data subjects based on their relationship with the controller... In any case, the existence of a legitimate interest would require a thorough assessment, including whether a data subject can reasonably foresee, at the time and in the context of the collection of personal data, that the existence of a legitimate interest would require a thorough assessment, including whether a data subject can reasonably foresee at the time and in the context of the collection of personal data. In particular, the interests and fundamental rights of the data subject could prevail over the interests of the controller when processing personal data in circumstances where the data subject does not reasonably expect further processing...*

*(58) The principle of transparency requires that all information addressed to the public or to the data subject must be concise, easily accessible, easy to understand, using clear and plain language and, where appropriate, 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 controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in*

*which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. If personal data are obtained from data subjects, they should also be informed of whether they are obliged to provide them and of the consequences if they do not do so...*

*(61) Information on the processing of their personal data should be provided to data subjects at the time when 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, inter alia, in its STC 39/2016 of 3 March, citing STC 292/2000 of 30 November, has established that the right to information is part of the essence of the right to data protection. Thus, in its FJ2 of STC 39/2016, it states:

*'The duty to provide prior information forms part of the essence of the right to data protection, since it is an indispensable complement to the person concerned's need for consent. The duty to provide information on the use and destination of personal data required by the Organic Law on the Protection of Personal Data is closely linked to the general principle of consent for the processing of data, since if the purpose and recipients of the data are not known, consent can hardly be given. Therefore, when assessing whether the right to data protection has been infringed as a result of a breach of the duty to provide information, the waiver of consent to data processing in certain cases should be a factor to be taken into account given the close link between the duty to provide information and the general principle of consent.*

*(...)*

*Thus, characteristic elements of the constitutional definition of the fundamental right to the protection of personal data are 'the rights of the data subject to consent on the collection and use of his or her personal data and knowledge thereof. In order to give effect to that content, recognition of the right to be informed of who possesses his personal data and for what purpose, and the right to be able to oppose such possession and use by requiring the relevant person to cease possession and use of the data, are indispensable. That is to say, by requiring the holder of the file to inform him of what data he has about his person, by accessing his appropriate records and entries, and what they have been intended for, which also extends to potential assignees; and, where appropriate, require you to rectify or cancel them" (STC 292/2000 of 30 November, FJ 7).'*

MIRACLIA does not at any time inform the data subject, i.e. the person who receives the call of joke, of the content of his or her rights as set out in the GDPR.This means that the data processing which it carries out cannot under any circumstances be regarded as lawful.

Article 12 (1) GDPR states that such information shall be provided "in writing"; only at the request of the data subject may the information be provided orally provided that the identity of the data subject is demonstrated by other means. In the present case, there has been no written information, nor has the identity of the person concerned been established by any means.

Article 13 (1) GDPR provides that 'where personal data relating to him or her are obtained from a data subject' (as is the case, since the call is made to the person who receives the call and therefore the personal data, his or her voice, comes directly from

the person who receives the call), the controller, 'at the time the data are collected', shall provide him with all the information set out below in that paragraph.

As can be seen from the facts of the case, MIRACLIA has not previously informed the person who receives the call of jokes of any of these circumstances, in such a way as to infringe the fundamental right to data protection of the person who receives the call from jokes, who have not been aware, prior to the recording which MIRACLIA always makes of their data in their systems, of the circumstances which the legislation lays down that they must be aware of.

The person concerned responds to a telephone call, which is to be recorded, not only without having been able to give his consent, but without having been informed, at that time, in such a way that he is aware of the intended processing of his personal data and of the circumstances required by the legislation protecting the fundamental right. These circumstances include the one provided for in Article 13 (1) (c) of the GDPR: the data subject must be informed at the time of obtaining his or her personal data, inter alia, of the legal basis for the processing, in addition to point (d), namely that where the processing is based on Article 6 (1) (f) — legal interest — the data subject must be informed of the legitimate interests of the controller or of a third party which are invoked as a legal basis for the processing.

That lack of information as to the legal basis for the processing or, in the case of a legitimate interest, what those legitimate interests are, is of great importance. The GDPR seeks to enable the data subject (the person who receives the call) to be aware at that time (at the time of collection of his or her personal data) of what legitimate interests are hypothetically invoked by the controller to process his or her personal data without the need for his or her consent. It is at this point that the controller must weigh up the legitimate interests which may be invoked by the controller against the interests or fundamental rights and freedoms of the data subject which require the protection of his or her personal data, in particular where the data subject is a child. Such a balancing exercise cannot be carried out at a later stage, unilaterally by the controller, without taking into account the rights, freedoms and interests of the person who receives the call of joke, since it is sufficient to say that he would be denied not only his right to information but also his right to make representations, to be heard in response to the controller's claim to use his personal data without his consent (that is precisely the effectiveness of the use of the legitimate interest as a legal basis for the processing, and what MIRACLIA claims as a controller).

The CJEU judgment of 29 July 2019, C-40/17, Fashion ID, sets out the guidelines as to who would in any event be required to seek the data subject's consent if there are two or more controllers. It also determines who is required to provide information to the data subject and when this information is to be given. It follows from that judgment that it would be for MIRACLIA to apply it to the present case.

Paragraphs 102 to 104 of the Fashion ID judgment state:

*'102 As regards the consent referred to in Articles 2 (h) and 7 (a) of Directive 95/46, it is apparent that consent must be given prior to the collection and communication by transmission of the data subject's data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent,*

*since it is the fact that the visitor consults that website that triggers the processing of the personal data. As the Advocate General noted in point 132 of his Opinion, it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means.*

*103 The same applies to the obligation to provide information laid down in Article 10 of Directive 95/46.*

*104 It is apparent from the wording of that provision that the controller or his representative must communicate to the data subject at least the information referred to in that provision. It follows that the controller must provide that information immediately, that is to say, at the time when the data are collected (see, to that effect, judgments of 7 May 2009, Rijkeboer, C 553/07, EU: C: 2009: 293-, paragraph 68, and of 7 November 2013, IPI, C 473/12-, EU: C: 2013: 715, paragraph 23).'*

As we know, there is no unlimited right and the right to information of the data subject, as an essential part of the fundamental right to the protection of his or her personal data, is not extraneous to that principle. However, as an exception, it must be interpreted strictly, so that it is only in the cases provided for by law that there can be an exception to the right to information.

As stated in paragraph 39 of the judgment of the Court of Justice of 7 November 2013, C-473/12, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others, to which we will refer more extensively:

*39 According to settled case-law, the protection of the fundamental right to privacy requires that exceptions to and restrictions on the protection of personal data be established within the limits of what is strictly necessary (judgments of 16 December 2008 in Case-73/07 Satakunnan Markkinapörssi and Satamedia ECR I-9831, paragraph 56, and judgment of 9 November 2010 in Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, ECR I 11063-, paragraphs 77 and 86).*

The only limitations to the right to information are to be found in Article 23 of the GDPR and express legislative measures are needed to agree on them, while respecting the essence of the rights and freedoms, and provided that the specific circumstances listed in that provision are met.

While referring to consent, MIRACLIA has pointed out that it is unable to comply with some regulatory provisions because the very fact of spending a joke or the surprise effect would be undermined. However, nothing has been put forward with regard to the limitations referred to, nor does they appear to be applicable in the present case. MIRACLIA does not mention any legislative measure that would lead to the possibility of derogating, in the case of the Juasapp application, from the fundamental right to the protection of the personal data of the data subject, the person called a joke, and therefore any subsequent analysis would be meaningless. In addition, the possibility to derogate by legislative measures from the fundamental rights of individuals is of such importance as state security, defence, public security, prevention, investigation, detection or prosecution of criminal offences etc. Therefore, such a possibility of exempting the data subject's right to information does not negate the possibility of spending jokes through

an online application, nor from a commercial interest, so that there can be no commercial interest justifying the right of the data subject to be informed in Article 13.

Therefore, MIRACLIA's action is not excluded from the obligation to provide data subjects with the right to information, with the content laid down in Article 13 GDPR, at the time when the personal data are obtained from the data subject. Where personal data are obtained from the data subject under no circumstances can that information be provided later, let alone never be the case, as is the case here. In short, the data subjects must in any event be informed so that the processing can be considered lawful, which has certainly not been the case.

The same applies to compliance with Article 14 GDPR, which governs the information to be provided to the data subject when the data are not collected directly from the data subject, as is the case in relation to the mobile telephone number of the person receiving the call, which is provided to MIRACLIA by a third party, the bromist.

In general, MIRACLIA does not provide MIRACLIA to the data subject/data subject (a person called a joke) in the documents 'Terms and Conditions of Use of the Service' and 'Privacy Policy', apart from indicating that 'Miraclia does not collect data from the recipients of the jokes', which, as we have seen, is not true.

The only information addressed to the person receiving the funeral call results from the expression reproduced at the end of the joke call, with the following message:

*"A friend of his own has spent a joke. If you do not want your friend to listen, download or spread the joke, or if you do not want to receive more jokes, click 5 with your keyboard after the signal. Beeep'.*

As can be seen, that term does not specify that the joke has been recorded and that, by the indicated action, it is removed from the institution's systems. Otherwise, the detail on none of the aspects set out in Articles 13 and 14 GDPR is included.

Moreover, at no time during the telephone conversation identifies the Juasapp application as the call manager or the developer MIRACLIA as owner of the platform, so that the receiver of the joke does not know where to contact to obtain more information about the call or to exercise its rights; at no time is the bromist named; nor is it reported at any time, during the course of the joke, that the conversation is being or may be recorded.

The facts set out above therefore constitute a breach of the principle of transparency laid down in Articles 13 and 14 of the GDPR, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of that Regulation.

Finally, it should be noted that MIRACLIA has argued that, in the course of these proceedings, which was aware of the complaint made for the first time in relation to the information defects, it immediately remedied it by supplementing the information provided at the end of the conversation of the joke as follows:
That someone has spent a joke to pass a good story.
The Juasapp application owned by MIRACLIA TELECOMUNICACIONES, S.L.

— To object to such a joke reaching the bromist and to remove it, you can click on key 5.
— You have more information by clicking on key 1.

Clicking on key 1 provides the detailed explanation, also included on the website. Thus, of the information which it did not provide to the data subject, it has now included: The identity of MIRACLIA
— the contact details of the Data Protection Officer
— The retention period
— The basis for locus standi
— The exercise of the full rights guaranteed by opposition and deletion rights (and also access rights when requested) are now formally specified.

It does not, however, provide any evidence to that effect; not even the text or recording of the word inserted at the end of the conversation, so that the alleged information given can be properly assessed. Nor does MIRICLIA state anything about the precautions taken to ensure that the person concerned has actually accessed the information or the measures to be applied in cases where communication is interrupted before the word is reproduced.

VIII

On the otherhand, Articles 6 and 7 GDPR refer, respectively, to 'Lawfulness of processing' and 'Conditions for consent':

*Article 6 GDPR.*

*'1. Processing shall be lawful only if at least one of the following conditions is met:*

*(a) the data subject gave his or her consent to the processing of his or her personal data for one or more specific purposes;*

*(b) processing is necessary for the performance of a contract to which the data subject is a party or for the implementation at the data subject's request of pre-contractual measures;*

*(c) processing is necessary for compliance with a legal obligation applicable to the controller;*

*(d) processing is necessary to protect the vital interests of the data subject or of another natural person;*

*(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

*(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.*

*Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.*

*2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.*

*3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:*

*(a) Union law; or*

*(b) the law of the Member States applicable to the controller.*

*The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data being processed; the data subjects concerned; the entities to which personal data may be disclosed and the purposes of such communication; the purpose limitation; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX.The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.*

*4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:*

*(a) any relationship between the purposes for which the personal data were collected and the purposes of the intended further processing;*

*(b) the context in which the personal data were collected, in particular as regards the relationship between data subjects and the controller;*

*(c) the nature of the personal data, in particular where special categories of personal data are processed in accordance with Article 9 or personal data relating to criminal convictions and offences in accordance with Article 10;*

*(d) the possible consequences for the data subjects of the intended further processing;*

*(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation'.*

Article 7GDPR.

*'1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

*2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

*3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent*

*before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.*

*4. In assessing whether consent has been freely given, the utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is subject to consent to the processing of personal data which are not necessary for the performance of that contract.'*

Account is taken of recitals (32), (39), (40) to (44) and (47) of the GDPR in relation to the above Articles 6 and 7.

Account should also be taken of the provisions of Article 6 of the LOPDGDD:

*'Article 6. Processing based on the consent of the data subject*
*1. In accordance with Article 4 (11) of Regulation (EU) 2016/679, the data subject's consent means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject agrees, either by a statement or by a clear affirmative action, to the processing of personal data relating to him or her.*
*2. Where it is intended to base the processing of the data on the consent of the data subject for a number of purposes, it must be stated specifically and unequivocally that such consent is given for all of them.*
*3. Performance of the contract shall not be subject to the data subject's consent to the processing of personal data for purposes other than those relating to the maintenance, development or control of the contractual relationship.'*

According to the above, data processing requires the existence of a lawful legal basis, such as the consent of the data subject validly given, where there is no other legal basis referred to in Article 6 (1) GDPR or the processing pursues a purpose compatible with that for which the data were collected.

Article 4 GDPR defines 'consent' in the following terms:

*"Article 4 Definitions*
For the*purposes of this Regulation the following definitions shall apply:*
*11.'the data subject's consent'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'*

Consent is understood as a clear affirmative act reflecting a freely given, specific, informed and unambiguous indication of the data subject's wishes to consent to the processing of personal data concerning him or her, provided with sufficient safeguards to establish that the data subject is aware of and to what extent consent is given. And should be given for all processing activities carried out for the same purposes or purposes, so that, where the processing has several purposes, consent should be given to all of them in a specific and unambiguous manner, without making the performance of the contract conditional upon the data subject's consent to the processing of his or her personal data for purposes which are not related to the maintenance, development or

control of the contractual relationship. In that regard, the lawfulness of the processing requires that the data subject be informed of the purposes for which the data are intended (informed consent).

Consent must be freely given. It is understood that consent is not freely given where the data subject has no real or free choice or cannot refuse or withdraw his or her consent without prejudice; or where it is not allowed to authorise separately the different processing operations of personal data despite being appropriate in the specific case, or where the performance of a contract or service is dependent on consent, even if the consent is not necessary for such fulfilment. This is the case where consent is included as a non-negotiable part of the general terms and conditions or when there is an obligation to agree to the use of personal data additional to those strictly necessary.

Without these conditions, giving consent would not give the data subject real control over his or her personal data and their destination, and this would render the processing activity unlawful.

The Article 29 Working Party discussed these issues in its "Guidelines on consent under Regulation 2016/679", revised and approved on 10/04/2018; it has been updated by the European Data Protection Board on 04/05/2020 through the document "Guidelines 05/2020 on consent under Regulation 2016/679".From what is stated in this document, it is now important to highlight certain aspects relating to the validity of consent, in particular concerning the 'specific', 'informed' and 'unambiguous' elements:

*< < 3.2. Specific*
*Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them. The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed 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 for 'granularity' to obtain 'free' consent. In sum, to comply with the element of 'specific' the controller must apply:*

*(I) the specification of the purpose as a guarantee against misuse;*
*(II) dissociation in requests for consent; and*
*(III) a clear separation between information related to obtaining consent for data processing activities and information on other matters.*

*Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity. The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.*
*Where the controller relies on Article 6(1)(a), data subjects shall always give their consent for a specific purpose for the processing of the data. In line with the concept of purpose limitation, Article 5(1)(b) and recital 32, consent may cover different operations, provided that such operations have the same purpose. It goes without saying that*

*specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.*
*Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data on the basis of consent and, in addition, wishes to process such data for another purpose, he or she must obtain consent for that other purpose, unless there is another legal basis that better reflects the situation...*
*(II): consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'.This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes. ad.*
*(III): lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement for controllers to provide clear information, as explained above in section 3.3 > >.*

*< < 3.3. Informed*
The*GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.*
*The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.*

*3.3.1. Minimum content requirements for consent to be 'informed'*
For consent to*be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:*
*(I) the identity of the controller;*
*(II) the purpose of each processing operation 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 decision-making in accordance with Article 22(2)(c), where relevant; and*
*(VI) information on the potential risks of data transfer due to the absence of an adequacy decision and adequate safeguards as described in Article 46 > >.*

In the present case, MIRACLIA claims in its submissions that consent cannot be the legal basis for spending a joke, thus taking the view that the processing of the personal data of the persons called by them is based on the legitimate interest of Article 6 (1) (f) GDPR.

However, that is not the case with the information contained in the document entitled 'Terms and Conditions of Use of the Service' (Second Proposed Event), in which it is stated on three occasions that the user must have the explicit and unequivocal consent

of the person who has received the joke so that the recording can be made and the audio file can subsequently be shared, as a requirement for the operation of the service ('The functioning of the service avoids the creation of a prior registration).In that document, MIRACLIA expressly states that 'it is not liable for the consequences of failure to obtain the consents necessary to share the recording'.

In other words, MIRACLIA bases the processing of personal data directly on the consent of the 'person called a joke', who must be collected by the 'bromist' himself.

MIRACLIA is aware, then, that that legal basis for the processing is purely formal, fictitious. If he considers that a joke can never be based on the consent of the person who receives the joke call, he does not understand what is stated in his document, knowing that the bromist will never seek the consent of the person receiving the call.

Moreover, the processing of personal data carried out by the data controller MIRACLIA cannot under any circumstances be regarded as 'lawful' since the data subject is not provided with the information to which he or she is entitled under the rules on the protection of personal data, as concluded in the earlier legal basis.

Nor can it be regarded as lawful where, in the absence of such information, the data subject is deprived of his right to know the legal basis for the processing alleged by the controller, and in particular, by referring to the legitimate interest, he is deprived of his right to know what those legitimate interests invoked by the controller or a third party would justify the processing without taking his consent into account.

Similarly, the data subject is deprived of his right to rely on the grounds on which that legitimate interest relied on by the controller could be counterbalanced by the rights or interests of the data subject. If the data subject had not been given an opportunity to rely on them against the controller, any balancing carried out by the controller without taking into account the circumstances which could be invoked by the data subject who was not allowed to do so would be vitiated by an act contrary to a mandatory rule.

If the rule requires the subject to be informed of his or her rights, and it is not done, the consequence must be the nullity of subsequent acts (the same balancing exercise would be vitiated by nullity of the right and the same processing of personal data carried out against a weighting which is null and void).

Moreover, there is no legal measure that derogates from that obligation to provide the information in question by the person responsible, as explained above.

Therefore, the legitimate interest referred to in Article 6 (1) (f) GDPR cannot be regarded as applicable as the legal basis for the processing of personal data.

However, although we consider that the legitimate interest is not applicable, it is necessary to analyse hypothetically the terms in which the balancing provided for in that article between the legitimate interest of the data controller and the protection of the data subject's personal data should be carried out, that is to say, how that legitimate interest, if applicable, is to be carried out.

However, if this were the case, the CJEU, already in its judgment of 4 May 2017,

C-13/16, Rigas Satskime, paragraphs 28 to 34, determined the conditions under which processing may be lawful on the basis of legitimate interests. The judgment of the Court of Justice of 29 July 2019 in Case C-40/17 Fashion ID, echoing the aforementioned judgment, sets out these requirements.

*28 In that regard, Article 7(f) of Directive 95/46 — (now Article 6 (1) (f) GDPR) — lays down three cumulative conditions for the processing of personal data to be lawful:first, that the controller or the third party or third parties to whom the data are disclosed pursue a legitimate interest; Second, that the processing is necessary for the purposes of that legitimate interest and, third, that the fundamental rights and freedoms of the data subject are not overridden by the data protection.*

Asregards the first of the conditions, namely that the controller or third parties pursue a legitimate interest, we are faced with a commercial interest, which could be regarded as legitimate in itself, namely to earn money by selling money to third parties. However, those benefits are obtained at the expense of affecting the rights and legitimate interests to the protection of their personal data of the data subjects (the person called upon to do so), and that interest must therefore be weighed against that of individuals.

As far as the second of the conditions is concerned, however, we consider that the processing of personal data carried out by the appellant is not necessary or strictly necessary for the fulfilment of his legitimate interest (paragraph 30 of the judgment of 4 May 2017, Rigas Satskime, C-13/16, states: 'As regards the requirement that data processing be necessary, it should be recalled that exceptions and restrictions to the principle of the protection of personal data must be established within the limits of what is strictly necessary').

This principle that processing must be strictly necessary for the purposes of legitimate interests must be interpreted in accordance with Article 5 (1) (c) GDPR, which refers to the principle of data minimisation, stating that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Apart from, as we have already mentioned, the fact that the data subject/person receiving the call does not know for what purposes or on what legal basis his data were collected, it is understood that the recording of the voice of the data subjects in the MIRACLIA systems, which is carried out in any event and in all circumstances, and also, as has been shown in the administrative file, that the telephone numbers of the data subjects are stored in these systems until the call is made, amounts to processing. If the legitimate interest pursued is charging for a person, the bromist, to be able to spend a joke, it does not seem necessary, as an intrinsic requirement of such processing, (i) to keep the personal data (telephone and voice).Nor can it be considered legitimate, and we therefore consider that it would be excessive treatment, that the bromist may (ii) download the voice of the person who receives the call of joke in order to be able to go to the recording as many times as he wishes and be able to disseminate it without restriction, so that (iii) security measures would also be lacking to prevent such further processing by the bromist. If the intention of MIRACLIA, with a purely commercial interest, is to charge for spending a joke, that processing could be done without the need to record the voice or telephone number, and without having to give the possibility, omnimod and unlimited, to the bromier to download from his terminal the voice of the

person receiving the call, so that it can subsequently be broadcast without limitation. The second condition relating to non-excessive or necessary use would therefore not exist.

Thirdly, as regards balancing or balancing, i.e. that the fundamental rights and freedoms of the data subject in data protection do not prevail, the CJEU has taken the view (Rigas Satskime) that it depends on the circumstances of the individual case in question.

In relation to this balancing exercise, the Working Party on Article 29 of Directive 95/46 issued Opinion 06/2014 on the concept of legitimate interests of the controller. In its opinion, the Working Party 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 those concerned are duly taken into account. At the same time, it is a scalable test, which can vary from simple to complex, and does not need to be unduly burdensome.*

The *factors to be considered when carrying out such a balancing test shall include:*

*— the nature and source of the legitimate interest, and whether the processing of data is necessary for the exercise of a fundamental right, is otherwise in the public interest or benefits from the recognition of the community concerned;*

*— the impact on the data subject and his reasonable expectations as to what will happen to his or her data, as well as the nature of the data and the way in which they are processed;*

*— additional safeguards that could limit an undue impact on the data subject, such as data minimisation, privacy technologies, increased transparency, the general and unconditional right to opt-out and data portability.*

(a) As regards the nature and source of the legitimate interest alleged, this is an interest of a commercial nature, as has already been shown. The TS, in its judgment in STS 1921/2017 of 5 May 2017, ECR 407/2016, has already pointed out that the interest of gas traders cannot prevail over the interests of consumers holding electricity supply contracts, since the latter have a fundamental right against a purely commercial interest, with the result that the person, the consumer in this case, has the legal power to impose on third parties the duty to refrain from interfering in their immediate sphere and prohibit them from making use of the and known judgments (citation 73/1982, citation 89/1987).

(b) It should be added, following the list of recommended balancing requirements, that the processing of data which the appellant seeks to carry out is by no means necessary for the exercise of a fundamental right and must therefore fall in the light of the need for data subjects to protect their fundamental right.

(c) Nor can the processing of personal data proposed by MIRACLIA be considered to be in the public interest or to benefit from the recognition of the community concerned.

(d) As regards the reasonable expectations of the data subject as to the use of his or her personal data and the implications for him, it is sufficient to mention that, with the processing of personal data which the appellant intends to carry out, the data subject loses any power of disposal over the data, since the data are recorded by a system,

before being able to give consent or even being informed, so that the broadest user would not be able to make use of the personal data of the person receiving the call, his or her voice, downloading it into his/her own terminal and further disseminating it, and thus the user would not be able to make use of the personal data of the person receiving the call, his or her voice, downloading it into his/her own terminal and further disseminating him/her.

(e)As regards the nature of the data, we consider that voice is particularly sensitive. This is because we all know that the voice uniquely identifies a subject from a wider or smaller community. But for the sake of completeness, voice can also be considered as sensitive data in another sense, and is that the GDPR allows voice to be considered a biometric data, provided that techniques aimed at enabling a natural person to be uniquely identified (Article 9.1 GDPR) are applied to it or can be applied to it. It does not appear that the data processing which the controller intends to carry out with the Juasapp application is intended to apply to the voice processing which makes it a biometric data, but even if that is not the purpose of the data processing carried out by the controller, there is no doubt that voice can constitute the raw material, the raw data, from which a technique could be applied to make that personal data, the voice, a biometric data. As the TS has had occasion to consider in the above-mentioned STS judgment 1921/2017 of 5 May 2017, ECR 407/2016, the criterion of 'risk' is a criterion to be taken into account when personal data, together with others, and in breach of the principle of information or access, may lead to the identification of the data subject.

(f)As regards the last of the above-mentioned weighting criteria, namely the additional safeguards that could limit an undue impact on the data subject, such as data minimisation, privacy technologies, increased transparency, we consider that it is absolutely necessary to increase transparency in terms of providing potential callers, in advance of the registration of their voice or telephone, with all the circumstances referred to in Article 13 GDPR.In addition, recording the voice of the person who receives the call of jokes in the appellant's systems is considered excessive within the meaning of Article 5.1 (c) GDPR.

In short, and in order to put an end to this point, it does not follow from the processing of personal data carried out by MIRACLIA that, beyond its own commercial interest, there are no circumstances justifying the recording of the voice of the persons called by jokes using the legitimate interest of Article 7 (f) of the Directive as the legal basis for processing. The processing of personal data carried out by MIRACLIA is not necessary for the purposes of the protection of a legitimate interest, nor does the legitimate interest of the appellant outweigh the fundamental rights and freedoms of the data subject in the protection of his or her personal data.

Consequently, the processing of personal data carried out by MIRACLIA cannot be considered to be covered by the legitimate interest provided for in Article 6 (1) (f) GDPR.Nor does the data subject give his consent to such data processing, which, moreover, is unlawful because the data subject's right to information as provided for in the legislation on the protection of personal data has been completely disregarded.

In accordance with the above, the above facts constitute a violation of Article 6 GDPR, which results in the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 GDPR.

IX

In its observations on the motion for a decision, MIRACLIA points out that the arguments contained in the previous legal grounds are not valid for Juasapp, which is in a different technical and data-processing context from that presented in previous actions of the Agency and ordinary justice. In the present case, according to MIRACLIA, 'Juasapp' complies with the definition of number-based interpersonal electronic communications services as defined in Article 2 (5) and (6) of Directive (EU) 2018/1972 establishing the European Electronic Communications Code (recast).

On the basis of this consideration, MIRACLIA understands that it is only by providing the necessary means to provide the service contracted by the user, which is the sole controller of the data of the person receiving the call; whereas the conversation which takes place in connection with the provision of the service is personal or household, in so far as the purpose of the service is to establish a communication initiated by the bromist, with MIRACLIA merely providing the means for transmission; it does not process the data of the recipient of the so-called 'joke' beyond compliance with the retention obligations laid down in Law 25/2007 on the retention of data relating to electronic communications and public communications networks.

For the same reason, MIRACLIA considers that it is not obliged to provide the information referred to in the GDPR, as the provisions of Recital 173 and Article 95 of the GDPR apply in conjunction with Directive 2002/58/EC on privacy and electronic communications. According to that Article, the GDPR does not impose additional obligations on natural or legal persons in relation to processing in the framework of the provision of public electronic communications services in public communications networks in the Union in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC, and, according to that Directive, interpersonal electronic communications services based on public numbering resources may not be required to identify the call operator and the platform owner or to indicate where to obtain caller rights. The right of the user of the service not to identify himself or herself to record the call must also be respected.

These arguments must be rejected, since there is not yet any provision in national law transposing Directive (EU) 2018/1972, the deadline for transposition of which has not yet expired. In those circumstances, it cannot be said that its activity by means of the Juasapp application falls within a category of electronic communications services which, at present, does not exist in our legal system.

Furthermore, Article 95 GDPR, which prohibits the imposition of 'additional obligations on natural or legal persons in relation to processing in the context of the provision of public electronic communications services in public communications networks in the Union in areas where they are subject to specific obligations with the same objective set out in Directive 2002/58/EC', is not applicable to the present case, which is not among the Directives that will be repealed by Directive (EU) 2018/1972 with effect from 21/12/2020. This act does not refer to Directive 2002/58/EC and does not involve the imposition of specific obligations with the same objective pursued by this Directive.

In any event, it should be added that MIRACLIA bases these claims on the outcome of the audit carried out on the Juasapp application by a telecommunications engineer in July 2020, well after the period analysed by the Inspectorate of this Agency. Although the responsible entity states that the version of the audited application corresponds to the version in force at the time when the complaints were made, there is no evidence to support this. In addition, that argument, if any, was raised in its submissions to the opening of the procedure and represents a different approach to the position which MIRACLIA has maintained during the previous stages, in which it showed its readiness to remedy some of the shortcomings identified and defended the legitimate interest of the entity in the processing of data which it carries out.

Moreover, it is based on assumptions and has established facts which cannot be accepted, mainly those relating to the existence of a conversation between a user of 'Juasapp', who initiates it, and a third party. It is stated that "the person initiating the conversation should be the user contracting the Juasapp service" and that "once the connection between the Juasapp user and the recipient of the conversation has been established, the direct exchange of interpersonal information through electronic communications networks between the two is allowed".However, it is common ground that the user of the application merely a call, in which he does not participate, which is made from MIRACLIA systems for the purpose of reproducing to the addressee a word (that corresponding to the joke selected by the user), with the result that there is no 'direct exchange of interpersonal information'.In the event of a call between the user and the recipient of the joke, that conversation would never take place with the intermediation of 'Juasapp'.

Similarly, it cannot be accepted that the user of 'Juasapp' decides to record the content of the message which he publishes himself. The 'joke' call remains in any case in MIRACLIA's systems, without it being necessary to involve the Juasapp user, who merely uses the means provided by the entity itself to access the audio file generated by the system, without the user taking any action to edit its content.

On this point, the approach set out in the audit report provided by MIRACLIA, according to which the qualification as an electronic communications service included in the Conditions of Use of the Application implies an implicit recognition of the nature of the service (Annex II to the audit report states verbatim as follows: 'In the conditions of use of the JUASAPP application it is stated in Article 6 that 'like any telecommunications service, the use of JUASAPP services for the purpose of harming or harming nobody is illegal'.There is therefore a contractual declaration that JUASAPP is a service subject to telecommunications regulation and thus an implicit acknowledgement that it is an electronic communications service in such a case").

It is clear that the position held by MIRACLIA as regards the functioning of the Juasapp application cannot be determined by an agreement between individuals or a contractual declaration, but by the legal determinations that are applicable.

It may even be said that those arguments must be rejected even if we consider the provisions of the European Electronic Communications Code, which defines interpersonal communications services to include the conveyance of signals and other types of services enabling communication. It distinguishes "three types of services which

may partially overlap, namely: Internet access services as defined in point (2) of Article 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council (1); interpersonal communications services as defined in this Directive and services consisting wholly or mainly in the conveyance of signals" (Recital 15 of Directive (EU) 2018/1972 establishing the European Electronic Communications Code).

According to Article 2, 'Definitions', for the purposes of that directive:

*< < The following definitions shall apply:*

*(4) 'electronic communications service' means: services normally provided for remuneration through electronic communications networks, which include, with the exception of services providing or exercising editorial control over content transmitted using electronic communications networks and services, the following types of services:*

*'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;*

*interpersonal communications service; and*

*services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;*

*(5) 'interpersonal communications service' means: generally provided in return for a direct, interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, where the initiator of or participant in the communication determines the recipient (s) and does not include services that enable interpersonal and interactive communication as a mere secondary possibility which is intrinsically linked to another service;*

*(6) 'number-based interpersonal communications service' means: an interpersonal communications service which either connects or allows communications with assigned public numbering resources, i.e. a number or numbers in national or international numbering plans, or allows communication with a number or numbers in national or international numbering plans; > >.*

With regard to these definitions, account should be taken of recitals 17 and 18 of that directive:

*(17) Interpersonal communications services are services which enable interpersonal and interactive exchange of information and include services such as traditional voice calls between two people, as well as all types of e-mails, messaging services or group talks. Interpersonal communications services only cover communications between a finite, that is to say not potentially unlimited, number of natural persons which is determined by the sender of the communication. Communications involving legal persons should fall within the scope of the definition where natural persons act on behalf of those legal persons or are involved at least on one side of the communication. Interactive communication entails that the service allows the recipient of the information to respond. Services which do not meet those*

*requirements, such as linear broadcasting, video on demand, websites, social networks, blogs, or exchange of information between machines, should not be considered as interpersonal communications services. In exceptional circumstances a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms 'minor' and 'purely ancillary' should be interpreted narrowly and from an objective end-user's perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service.*

*(18) Interpersonal communications services using numbers from a national and international numbering plan connect with publicly assigned numbering resources. Those number-based interpersonal communications services comprise both services to which end-users numbers are assigned for the purpose of ensuring end-to-end connectivity and services enabling end-users to reach persons to whom such numbers have been assigned. The mere use of a number as an identifier should not be regarded as equivalent to the use of a number to connect with publicly assigned numbers and should therefore not be considered sufficient in itself to qualify a service as a number-based interpersonal communications service. Number-independent interpersonal communications services should be subject to obligations only where public interests require that specific regulatory obligations apply to all types of interpersonal communications services, regardless of whether they use numbers for the provision of their service. It is justified to treat number-based interpersonal communications services differently, as they participate in, and hence also benefit from, a publicly assured interoperable ecosystem.*

Therefore, a number-based interpersonal electronic communications service should allow for a direct, interpersonal and interactive exchange of information between persons, without such interpersonal and interactive communication being included in the service concerned as a mere secondary possibility.

Consequently, MIRACLIA is not a provider of electronic communications and networks and does not provide electronic communications services.

Moreover, for the reasons set out above, this Agency considers that the doctrine of the Constitutional Court relied on by MIRACLIA, which allows the recording of a personal conversation by one of the participants, is not applicable to the present case. Nor does it consider that the present case gives rise to any controversy affecting the citizens' right to freedom of expression.

MIRACLIA also points out, in its submissions on the draft decision, that MIRACLIA is wrong to find that MIRACLIA is the owner of a mobile application known as 'Juasapp', indicating that it is a service accessed by means of a mobile app. However, in relation to this issue, we refer to the many references in the document "Terms and

Conditions of Use of the Service" on the "Juasapp" application (e.g.: 'Definition of the service: Juasapp is an application...").

It also considers that the reference to the hosting of the jokes on a public site is incorrect in so far as access to the audio is made via a private URL to which only the sender of the joke and the recipient of it have access, if he so wishes. However, according to MIRACLIA, what is stated in MIRACLIA is not contrary to what is stated by MIRACLIA when it states that there is 'no platform on which the gumps are published in order to be accessible to any third party, but the recordings of the jokes are hosted on a public site, which makes it possible for them to be accessed by means of the link to the audio file, which can be disseminated indiscriminately by the bromist user'.

With regard to the findings made in 5, it is claimed that the link accessed by the Agency's inspection services to check that 'Juasapp' operates in other countries of the European Economic Area corresponds to a pre-production platform that has never worked. However, according to the Inspectorate, access was made from the Agency's own offices to information that was in production on that day, available to any third party user of the network, that is to say, publicly available information. The Inspection Services have not provided any access to MIRACLIA systems under development. In any event, this entity does not dispute the information contained in the aforementioned Probation Event on the functioning of the Juasapp application in the countries indicated and the availability to the public of the terms and conditions of use in the languages mentioned.

With regard to the complaints set out in the Background, MIRACLIA repeatedly warns that it should not be admissible, bearing in mind that the respective complainant did not first address the organisation in exercising the rights conferred by the legislation on the protection of personal data.

In thisregard, on the one hand, it should be noted that, in the exercise of its powers and prerogatives, the Agency determined as the subject of the proceedings the overall analysis of the Juasapp application from the point of view of the rules on the protection of personal data and in relation to the persons receiving the calls, irrespective of the specific incidents of the complaints raised, which served to motivate the initiation of appropriate investigations into the processing of the personal data of the persons receiving the calls, regardless of the specific incidents of the complaints raised, which served to justify the initiation of appropriate investigations into the processing of the personal data of the persons receiving the calls; on the other hand, the exercise of those rights is not established as a necessary budget in order to be able to lodge a complaint with this Agency. The decision whether or not to lodge such a complaint or the use of any other means for the defence of his or her rights is the sole decision of the complainant. In any event, it should be noted that the decision adopted is the result of the established facts and that no scope has been attributed to the questions raised by MIRACLIA in relation to the representations made by the complainants concerning the sending of the recording by whatsapp, the making of calls other than the call for jokes, the sending of emails or the attention given by MIRACLIA to requests for exercise of rights.

Unlike the present case, the precedent cited by MIRACLIA, which concerns the case of a person who received a funeral call from a radio station, concerns a claim for the protection of rights for failure to take care of the request for erasure of data which he had

previously submitted to the controller, and as such was dealt with by that agency.

Finally, MIRACLIA asks for a face-to-face hearing in order to clarify the points raised before the Agency's investigators/inspectors and warns that, if its interests are not met, it reserves the right to go to other higher or judicial bodies in Spain and Europe. Such a hearing is not provided for in the applicable procedural rules, with the result that there is no obligation to do so, nor does it undermine the rights of the defence of the entity concerned, which will obviously have the possibility of challenging the decision in all the avenues provided for by that legislation.

X

In the event of an infringement of the provisions of the GDPR, among the corrective powers available to the Spanish Data Protection Agency as a supervisory authority, Article 58 (2) of that Regulation provides as follows:

*"2 Each supervisory authority shall have all of the following corrective powers:*
*(...)*
*(b) sanction a controller or processor with warning where processing operations have infringed the provisions of this Regulation; "*
*(...)*
*(d) to order the controller or processor to comply with the provisions of this Regulation, where applicable, in a specified manner and within a specified time limit;*
*(...)*
*(I) impose an administrative fine in accordance with Article 83, in addition to or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case; ';*

Pursuant to Article 83 (2) GDPR, the measure provided for in point (d) above is compatible with the penalty consisting of an administrative fine.

XI

In the present case, it is established that MIRACLIA's processing of personal data is carried out without first informing the data subject and without standing to do so.

The data subject does not know whether his or her personal data are being processed by this entity, which uses an application designed to use personal data provided by a third party and by the data subject himself. The application is created for a purpose which requires the processing of personal data. Thanks to the app, the telephone line to which the communication is sent is processed, recorded and reproduced the conversation held by the interlocutors.

In accordance with the findings made, it is considered that the facts set out above could breach the principle of transparency laid down in Articles 12, 13 and 14 of the GDPR, as well as the principle of lawfulness of processing governed by Article 6 GDPR, which, if confirmed, could entail the commission of the two offences defined in Article 83

(5) GDPR, which, under the heading 'General conditions for imposing administrative fines', provides as follows:

*'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines of up to EUR 20 000 000 or, in the case of an undertaking, up to 4 % of the total overall annual turnover of the preceding financial year, whichever is higher:*

*(a) the basic principles for processing, including the conditions for consent under Articles 5, 6, 7 and 9;*

*(b) the rights of data subjects under Articles 12 to 22; (...)'.*

In that regard, Article 71 of the LOPDGDD provides *that '[t]he acts and conduct referred to in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 and those which are contrary to this Organic Law shall constitute* infringements'.

For the purposes of the limitation period, Article 72 of the LOPDGDD states:

*'Article 72. Infringements considered to be very serious.*

*1. In accordance with Article 83 (5) of Regulation (EU) 2016/679, infringements which constitute a substantial infringement of the articles referred to therein, and in particular the following, shall be considered to be very serious and shall be time-barred after three years:*

*(...)*

*(b) the processing of personal data without one of the conditions for the lawfulness of the processing laid down in Article 6 of Regulation (EU) 2016/679 being fulfilled.*

*(...)*

*(h) failure to inform the data subject of the processing of his personal data in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 and Article 12 of this Organic Law'.*

In order to determine the administrative fine to be imposed, the provisions of Articles 83.1 and 83.2 of the GDPR must be observed, which state:

*'1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 9 and 6 shall in each individual case be effective, proportionate and dissuasive.*

*2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2).When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*

*(a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation concerned as well as the number of data subjects concerned and the level of damage suffered by them;*

*(b) the intentional or negligent nature of the infringement;*

*(c) any action taken by the controller or processor to mitigate the damage suffered*

*by data subjects;*

*(d) the degree of responsibility of the controller or processor, having regard to the technical or organisational measures they have implemented pursuant to Articles 25 and 32;*

*(e) any previous infringement committed by the controller or processor;*

*(f) the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*

*(g) the categories of personal data concerned by the infringement;*

*(h) how the supervisory authority became aware of the infringement, in particular whether and to what extent the controller or processor notified the infringement;*

*(I) where the measures referred to in Article 58(2) have been previously ordered against the controller or processor concerned in relation to the same matter, compliance with those measures;*

*(j) adherence to codes of conduct under Article 40 or to certification mechanisms approved pursuant to Article 42; and*

*(K) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial profits gained or losses avoided, directly or indirectly, through the infringement."*

Article 76 'Penalties and corrective measures' of the LOPDGDD provides:

*'1. The penalties provided for in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 shall be applied taking into account the graduation criteria set out in paragraph 2 of that Article.*

*2. In accordance with Article 83 (2) (k) of Regulation (EU) 2016/679, account may also be taken of:*

*(a) the continued nature of the infringement;*

*(b) linking the offender's activity to the processing of personal data.*

*(c) the profits made as a result of the infringement.*

*(d) the possibility that the conduct of the person concerned might have led to the commission of the infringement.*

*(e) the existence of a merger by acquisition after the infringement has been committed, which cannot be attributed to the acquiring entity.*

*(f) the allocation to the rights of minors.*

*(g) provide, where this is not required, a data protection officer.*

*(h) referral by the controller or processor, on a voluntary basis, to alternative dispute resolution mechanisms in cases where there is a dispute between them and any data subject."*

In accordance with the provisions set out above, for the purpose of determining the amount of the fines to be imposed in the present case on the defendant, who is responsible for the offences referred to in Article 83 (5) (a) and (b) of the GDPR, the fine to be imposed for each of the alleged infringements should be graduated.

It is considered that, as aggravating factors, applicable to the two breaches of the GDPR for which MIRACLIA is held responsible, the following factors indicate greater unlawfulness or guilt in the conduct of the entity:

.The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operations concerned: the seriousness of the infringement is determined by the processing operations carried out by MIRACLIA itself, which include the collection of personal data in order to make them available to third parties, providing them with functionalities or tools for the dissemination of such personal data, even though their processing is contrary to the GDPR.The duration of the infringement, considering that it is linked to the very functioning of the Juasapp application, is determined by the period of operation of that application.

.The intentional or negligent nature of the infringement: this is the result of the very design of the application, which has in no way provided for compliance with the rules on the protection of personal data. This is a particularly significant aggravating factor, since, without any doubt, the applicant was aware of the shortcomings identified by the Agency in the operation of the application from a number of precedents, in which it was penalised for breach of the principle of consent. MIRACLIA does not ignore the fact that its conduct is in breach of the GDPR and decided to proceed with it.

.The continuing nature of the infringement: result of the uninterrupted operation of the Juasapp application.

.The link between the activity of the offender and the processing of personal data and benefits obtained as a result of the commission of the infringement: all the operations which constitute the commercial or commercial activity carried out by the respondent involve the processing of personal data, all of which are affected by the same breaches of the rules. Thus, all the profits of this business are the result and consequence of the permanent breach of data protection law for which the respondent is responsible.

.The volume of data and processing which is the subject of the dossier; and number of stakeholders: it is taken into account that the perceived defects in data processing affect all those who receive a joke call using the 'Juasapp' app.

.The nature of the damage caused to the persons concerned or to third parties: the damage that may result from the processing and dissemination of the data is unpredictable, without any caution being taken by MIRACLIA in this respect.

.The accused entity does not have adequate procedures in place for the collection and processing of personal data, so that the infringement is not the result of an anomaly in the operation of those procedures, but a defect in the personal data management system designed by the controller.

On the basis of the factors set out above, the initial assessment of the fine contained in the decision to initiate proceedings amounted to EUR 50,000 per house of one of the alleged infringements.

However, in its written pleadings, the undertaking requested a reduction in that fine, since it represents 25 % of its turnover, which amounted to EUR 476,000 in 2018, in which losses were incurred.

The financial information available for MIRACLIA relates to the year 2018, the last financial year submitted. There is a turnover for that financial year of EUR 475,823 and a profit or loss of EUR -7,364. It is also found that this is a micro-enterprise with 2 employees. According to the information in the Central Companies Register, the 'subscribed capital' amounts to EUR 6,000.

In view ofthis, it is considered appropriate to propose the imposition of a fine of EUR 20,000 for each of the infringements committed (infringement of the principle of transparency for non-compliance with Articles 13 and 14 of the GDPR, which is defined in Article 83 (5) (b)) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD; infringement for failure to comply with the provisions of Article 6 of the GDPR, as defined in Article 83 (5) (a) and classified as very serious for the purposes of prescription in Article 72 (1) (b) of the LOPDGDD].

XII

In accordance with Article 58 (2) (d) GDPR, each supervisory authority may "order the controller or processor to comply with the provisions of this Regulation, where appropriate, in a specific manner and within a specified time limit...".

In this case, having regard to the circumstances expressed in relation to the identified shortcomings in the functioning of the Juasapp application, from the point of view of data protection law, MIRACLIA should be required to comply, within a period to be determined, with the rules on the protection of personal data, the processing operations it carries out, the information provided to its customers and the procedure by which they give their consent to the collection and processing of their personal data; it also establishes mechanisms to establish that the data subject has effectively accessed the information provided and that he or she has given his or her consent to the collection and processing of the personal data. All of this is within the scope and in the sense expressed in the grounds of the present judgment.

In cases where the data subject was not duly informed about the circumstances covered by Articles 13 and 14 GDPR or the data subject did not consent, MIRACLIA will not be able to carry out the collection and processing of the personal data.

Moreover, it is appropriate that MIRACLIA cease the unlawful use of personal data contained in its information systems relating to data subjects who have not given their informed consent to that end.

These measures shall apply in all countries of the European Economic Area in which MIRACLIA operates through the Juasapp application and in respect of persons residing in those countries.

It should be noted that failure to comply with the requests made by that body may be regarded as a serious administrative infringement because it 'does not cooperate with the supervisory authority' in the light of the requests made, and such conduct may be assessed at the time of the opening of an administrative procedure leading to a fine.

Therefore, in accordance with the above, the Director of the Spanish Data Protection Agency DECIDES:

FIRST: On the basis of the complaint received through the IMI system referred to in Antecedente Seventh and in accordance with the facts and points of law contained in this act, adopt a draft decision on the penalty proceedings against MIRACLIA TELECOMUNICACIONES, S.L., which will lead, where appropriate, to the adoption of the following agreements:

1. Penalise the entity MIRACLIA TELECOMUNICACIONES, S.L., for an infringement of Articles 13 and 14 of the GDPR, which is defined in Article 83 (5) (b) and classified as very serious for the purposes of limitation in Article 72 (h) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).

2. Penalise the entity MIRACLIA TELECOMUNICACIONES, S.L., for an infringement of Article 6 of the GDPR, referred to in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (b) of the LOPDGDD, with a fine of EUR 20,000 (twenty thousand euros).

3. Require MIRACLIA TELECOMUNICACIONES, S.L to comply, within three months, with the rules on the protection of personal data, the processing operations it carries out, the information provided to its clients and the procedure by which they must give their consent to the collection and processing of their personal data, to the extent stated in Article XII of Law. This should also be implemented in all the countries of the European Economic Area in which MIRACLIA operates through the Juasapp application.

SECOND: In accordance with the procedure laid down in Article 60 of the GDPR, this draft penalty decision is transmitted through the IMI system without delay to the supervisory authorities concerned, informing them that, in the event that no objections are raised within four weeks of the consultation, the mandatory decision on the penalty procedure will be adopted, in which the infringements referred to in the grounds of law will be declared, with the imposition of the penalties and measures indicated.

**Communications**
According to Article 60.7 of the GDPR, as lead supervisory authority, the Spain-SA shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds.

The supervision authority with which a complaint has been lodged shall inform the complainant on the decision.

[redacted]
Chair of the Spain-SA