CNS 13/2018

Opinion in relation to the consultation of a City Council on the use of Whatsapp by a local administration

A letter from a City Council is presented to the Catalan Data Protection Authority, in which it raises several questions regarding the risks and responsibilities involved in the use of the Whatsapp application for certain purposes in the context of a local administration

The consultation raises the degree of adequacy to the data protection regulations in relation to different cases in which the possibility of using Whatsapp is being considered. These cases refer to communication with the parents of minor users of the municipal toy library; with communication between members of the Municipal Culture Council (councillors, members of municipal associations...); with communication between members of the Children's Council (councillors, minors, school representatives...); as well as in relation to a Whatsapp group allegedly created by a group of young people in the village.

The consultation asks, among other aspects, about the responsibility that the City Council could have in relation to the use of this communication channel, or about the consent that would need to be asked from the participants of the group.

Having analyzed the request, and seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

The City Council asks about the degree of adequacy to the data protection regulations in relation to different cases in which, according to the consultation, the City Council would be considering the possibility of using Whatsapp, specifically, in the following cases:

Case 1: A municipal Whatsapp group that would include parents of children using the municipal toy library, whose administrator would be a municipal worker using a municipally owned phone. According to the consultation, the purpose is the disclosure of events that take place in the toy library, changes to schedules, cancellations of events, etc.

Case 2: Whatsapp Group of the Culture Council, whose members would be its members (councillors, members of village associations...) and municipal staff, and the administrator of the Group would be the City Council. The purpose would be, according to the query, the sending of notices, cancellations, etc.

Case 3: Whatsapp group of the Children's Council, the members would be the members of the Council (councillors, minors school representatives...) and municipal staff, and the administrator of the Group would be the City Council . The purpose of which would be, according to the

consultation, sending invitations, cancellations, etc. In this case, the consultation highlights the peculiarity that minors would be included in the group.

With regard to cases 1, 2 and 3, the City Council raises the same doubts, referring, in short, to the consent of the people participating in the groups, or to the City Council's responsibility regarding the comments or data that the participants could to spread.

Case 4: Whatsapp group that, according to the inquiry, would have been created by village youth. The query does not provide information about the purpose of the Group. The consultation points out that the City Council is not the administrator of the Group, and that a municipal employee would have been added using a telephone number of the City Council itself. The consultation raises whether, as it is not an administrator of the group, the City Council would have any responsibility as a public administration, and whether it should carry out any management in relation to the LOPD (Organic Law 15/1999, of January 13, on the protection of personal data).

Given the consultation in these terms, we will refer jointly to Cases 1, 2 and 3 raised by the City Council, since they are substantially identical in terms of their characteristics (they are Groups created by the City Council itself to communicate information about services or municipal activities) and regarding the doubts they raise; separate reference will be made to Case 4, cited.

III

By way of introduction, it should be noted that the media or communication services that can be used by public administrations (in this case, a City Council), either to relate to citizens or to other public administrations, or as a channel of internal communication within its own structure, they can be many and of a very varied nature (traditional media (press, radio or television), Internet, websites of organizations and public bodies, corporate intranets, ordinary mail, communication by telephone , face-to-face communication, etc.

To the extent that the use of any media, channel or communication service by the City Council involves the processing of personal information, this processing must be subject to the principles and guarantees of data protection, that is to say, the 'RGPD, which entered into force on 25 May 2016, and which will be applicable from 25 May 2018 (art. 99 RGPD). It is also necessary to take into account, until the full entry into force of the RGPD on the indicated date, the provisions of Organic Law 15/1999, of December 13, on the protection of personal data (LOPD), and the Royal Decree 1720/2007, of 21 December, approving the LOPD Deployment Regulations (RLOPD).

From the moment that the City Council enables a communication channel with the citizens and/ or its workers or councillors, the processing of data of those affected or interested (art. 4.1 RGPD and art. 3.e) LOPD) that derivi must be subject to the principles and guarantees of the data protection regulations, in the terms of the aforementioned regulations.

Specifically, the City Council refers to the use of the instant messaging system (SMI) of Whatsapp. SMIs are channels of real-time communication between two or more people, primarily text-based, sent over devices connected to a network such as the Internet. These apps, like Whatsapp, or similar, allow you to attach text messages, and image files, video and

audio, that is, other content apart from the text message itself. In addition to using basic messaging, users of these systems can make video conferences, create more or less numerous groups (as would be the case with the Groups referred to in the query), "chats", and share information, files or contacts.

In any case, it is clear that creating a Whatsapp Group - or, by extension, other similar SMIs, of the many currently available on the market -, involves the processing of personal data. On the one hand, the personal identifying data of the members of the Group (names, pseudonyms used, mobile number, profile picture, etc.), and on the other, the personal information that may be contained in the messages that are sent, whether in writing, voice messages, images, etc.

Since this information refers to natural persons, it is personal information subject to the protection of the corresponding regulations (LOPD and RLOPD, until May 25, 2018, and RGPD, from May 25, 2018).

The Parliament of Catalonia has issued Resolution 280/XI, of the Parliament of Catalonia (BOPC 220, of 27 September 2016), on the use of communications services by the Government, according to which the Government is urged to promote the 'use of SMI, by Public Administrations, which have certain characteristics, among others, a privacy policy in accordance with current legislation on data protection, which practice transparency, and which incorporate the measures which establishes Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data, in accordance with the established deadlines.

We agree that this Authority has analyzed the use of SMI from the perspective of data protection on previous occasions as well as, specifically, the content of Resolution 280/XI, cited (Opinions CNS 24/2013, CNS 55/2016, or CNS 54/2017, to which we refer).

IV

According to article 4.7 RGPD (and art. 3.b) LOPD), is responsible for the treatment: "the natural or legal person, public authority, service or other organism that, alone or together with others, determines the ends and means of treatment; if the Law of the Union or of the Member States determines the purposes and means of the treatment, the person responsible for the treatment or the specific criteria for his appointment may be established by the Law of the Union or of the Member States;"

The person responsible for the file or treatment is the one who, in the first instance, is obliged to comply with the principles and guarantees of the protection of personal data.

When a public administration, such as a city council, has to process personal information of those affected for the fulfillment of its functions and powers, this administration is the first responsible for the files or the data processing it carries out. Thus, when the City Council exercises its functions in relation to the management of municipal spaces (such as a toy library), or in relation to municipal competences in the field of culture or children, among others, the processing of data that is generated in compliance with these municipal powers means that the City Council must ensure compliance with data protection regulations.

Therefore, the City Council will be responsible for the personal information it processes through any SMI or collects through this means.

Apart from this, the use of SMI by the Public Administrations is unique, given that it is the user himself (the natural person) who decides to install a certain instant messaging application, through which may be related to third parties, including, where appropriate, Public Administrations.

As this Authority has done in the past, the companies holding SMIs (such as Whatsapp) decide what treatment they do with the data of users who decide to use their messaging service, and those who establish the corresponding conditions of use. In the information that is usually made available to users through the respective websites (for the purposes they are concerned, www.whatsapp.com), these companies determine which information they will use and which they will not, including personal data of the user and of the user's contacts, and for what purposes.

From here, any SMI company that processes data from its users must also comply with the principles and guarantees of the data protection regulations, in the terms that correspond.

Certainly, it is the company responsible for the SMI that must guarantee that it complies with data protection regulations, but this is an issue that the City Council must also bear in mind when deciding to provide its services through 'a certain channel of communication. The City Council must ensure that the communication channel complies with the requirements of the regulations.

The City Council is responsible for processing personal data in relation to the use of the toy library, or in relation to the activity of the Culture or Children's Councils, among others, and as such is responsible for the information personal data that it collects from those affected (parents of the toy library, neighborhood representatives, school students, or from its own councilors and municipal workers), and from the subsequent treatment that is carried out.

For the purposes that concern, from the moment that the City Council assesses the possibility of creating a Group or an SMI chat (Whatsapp, or others similar) to communicate with those affected who will be part of the Group (citizens, councilors, municipal workers , etc), and thus manage a certain municipal activity or service, you must take into account that this will generate an information flow (of identifying and contact data of the rest of the members of each Group, and of the information that is shared in the Group , such as text or sound messages, images...), between participants, which must comply with the requirements of data protection regulations.

In this sense, we agree that there is a substantial difference between the different communications that the City Council can establish, in the case at hand.

On the one hand, nothing prevents the City Council from processing the data it has as responsible (for example, of the parents of the toy library), in order to establish a direct and two-way communication with them, for the fulfillment of legitimate purposes ; in this case there is no third-party access to the information that can be shared between the City Council and the affected person.

Now, if the City Council, as responsible for the personal data of those affected, processes the contact data to create a list of participants to create an SMI Group, it must have an adequate legal basis to carry out this processing, bearing in mind that in this case the information flow multiplies, since both the data of

contact and the content of the messages, will be available to all participants in the Group.

This obliges the City Council, when creating SMI Groups, to be particularly careful and to analyze a series of issues, such as the legal basis of the treatment, and the information it will have to give to the members of the Group, in order that the aforementioned information flow (among all Group participants) conforms to the requirements of data protection regulations.

Having made this general consideration, it must be said that Whatsapp, to which the query refers, is a company based outside the European Union. However, according to article 2.2 of the RGPD:

> "2. The present Regulation applies to the processing of personal data of interested parties who reside in the Union by a person in charge or manager not established in the Union, when the processing activities are related to: a) the offer of goods or services to those interested in the Union, regardless of whether they are required to pay, or (...)."

Therefore, when Whatsapp is used on user devices that, as in the case at hand, are located in Spain, the application of the principles and guarantees of the personal data protection regulations (LOPD, RLOPD, and RGPD) in the cases subject to consultation.

This Authority has highlighted on previous occasions several problems presented by the processing of data by some instant messaging companies, including - although not exclusively - Whatsapp, from the perspective of data protection.

There are various actions carried out in recent years by European data protection authorities in relation to the processing of user data in the EU by Whatsapp, such as the reports and investigations of various data protection authorities (Dutch Data Protection Authority and Canadian Federal Authority, January 2013). It is also necessary to remember the intervention of WG 29, through several writings addressed to Facebook and Whatsapp (October 27, 2016, December 16, 2016 and October 24, 2017), in which several deficiencies in the mechanism for providing user consent following the provision of data communication to Facebook, ("Facebook family of companies"), for a set of purposes that include marketing and advertising.

Among other issues, the principle of consent must be taken into account (art. 4 LOPD and art. 4.11 RGPD). It is notorious that several SMI companies, including Whatsapp, include general or standard conditions, set and modified unilaterally by the company, leaving no room for choice to the user. Although it may be reasonable that the user must necessarily accept a certain level of processing of his data to the extent that this may be necessary from a technical point of view for the provision of the messaging service, this does not imply that it is appropriate to provide a general and, we could say, "indiscriminate" consent, in the sense of an unconditional acceptance, to use the user's data or that of third parties for purposes that are not strictly necessary for the provision of the service.

In this sense, the RGPD (Recitals 32 and 43) establishes the relevance of granularity in the provision of consent, an element that is not new in the field

that concerns us, because it had already been expressly cited and recommended by GT 29, in its Opinion 2/2013, on apps on smart devices ("Opinion 2/2013, on apps on smart devices"), of February 27 of 2013, and reiterated by GT 29 in the document "Guidelines on Consent under Regulation 2016/679", of November 28, 2017.

As can be seen from the information available on the Whatsapp website ("Terms of Service of Whatsapp"): "Address book. You regularly provide us with the phone numbers of Whatsapp users and the other contacts you have in your mobile phone's address book." (...), it can be noted that Whatsapp does not apply a granular consent that allows the user to select the contacts to which they will have access.

On the other hand, as can be seen from the considerations and warnings from the European Data Protection Authorities in recent years and, more recently, from Resolution R/00259/2018, of the Spanish Data Protection Agency, in which Whatsapp is sanctioned for transferring personal data to Facebook without the appropriate consent of those affected, Whatsapp would not apply the parceled consent in relation to the transfers of user data to third parties, and would not have allowed those affected to exclude certain personal information from said transfers to Facebook, which according to the recent opinions and resolutions of various Data Protection Authorities, would be clearly unnecessary transfers and, therefore, should have been subject to the users' consent.

It should also be taken into account that the RGPD gives the principle of transparency a letter of nature (consideration 39 and consideration 58 RGPD). According to article 5.1.a) of the RGPD, the data must be treated lawfully, loyally and transparently in relation to the interested party. The principle of transparency, linked in the RGPD to the principles of legality and loyalty, specifically includes the right to inform those affected about a series of issues, in the terms of article 13 RGPD (which in some aspects goes beyond of the provisions of article 5 LOPD), which collects the information that the person in charge, in this case the company responsible for an SMI, in this case Whatsapp, should give to the affected person, also in a granular way and for layers ("layered and granular information"). As this Authority has done in advance, not only Whatsapp, but also other SMIs of fairly common use, could present deficiencies in terms of compliance with the requirements of Article 13 RGPD, in short, of the information they provide to their users .

Finally, the third consideration that, without intending to be exhaustive, should be taken into account regarding the processing of user data by Whatsapp (to which the query specifically refers and to which, therefore, we refer), is located in the scope of the applicable security.

Among other issues, as this Authority has agreed (FJ VIII Opinion CNS 24/2013; FJ X Opinion CNS 55/2016), the forecasts that can be made explicit by the responsible companies (in this case, Whatsapp), regarding confidentiality with those that deal with user data (information encryption measures, etc.), are particularly relevant. In any case, we note that the RGPD, applicable from May 25, 2018, configures a security system that is not based on the basic, medium and high security levels (according to the scheme of the LOPD and RLOPD), but by determining, following a prior risk assessment, which security measures are necessary in each case, taking into account the type of information processed (Consideration 83, and arts. 24.1 and 32.1 RGPD). In the article "WhatsApp rolls out end-to-end encryption to its over one billion users", by the EFF Organization, available in Spanish translation: https://www.eff.org/es/deeplinks/2016/ 04/whatsapp-releases-end-end-encryption-for-mas-

of-a-billion-of-users), WhatsApp's encryption system is analyzed, which qualifies as a strong system.

From the information available (including its website), Whatsapp incorporates end-to-end encryption, so that only the sender and receiver (and not Whatsapp) can read the message. This type of encryption would be enabled by default for all users using the latest versions of the app, and could not be disabled. Now, according to other available information, while Whatsapp's end-to-end encryption offers guarantees, certain shortcomings are also detected that could lead to these measures not being sufficiently operational. Specifically, the Amnesty International (AI) report: “For your eyes only?. Ranking 11 technology companies on encryption human rights" (https://www.amnesty.org/download/Documents/POL4049892016ENGLISH.PDF) and Whatsapp does not encrypt that user, if backup copies are made in the cloud, this information it would not be encrypted. In short, there are vulnerabilities detected - not only in Whatsapp but in other SMIs available on the market - that should be taken into account, not only by the users themselves who install instant messaging apps, but, logically, the Public administrations that want to use it.

For all the above, and without prejudice to some shortcomings, from the perspective of data protection, in relation to the principles of data protection and the specific problem that a certain SMI (in this case, Whatsapp) can represent in relation to the data processing of the users of these SMIs, which the Administrations must take into account, in the case in question it is key to contextualize the possibility of creating and using Whatsapp Groups in the cases raised, with attention to type of information that, presumably, and given the information available, could be treated, and for the intended purpose.

v

When a City Council, as responsible (art. 4.7 RGPD), wants to use an SMI for its communications with citizens, it must take into account, at the outset, what type of communication it wants to establish, in relation to which service or provision, to which people or groups is the information or service in question addressed, what type of information will be affected, etc.

From the perspective of data protection, it does not have the same implications to use communication channels with citizens in order to provide information or receive inquiries on various issues (information on the state of traffic, or on certain municipal services, on activities recreational or cultural, etc...), which involves a flow of information that we could describe as general or "innocuous", that the use of SMIs to communicate a possible criminal act, an accident (communications to police forces, services healthcare, ambulances, services for dependent people who require home care, etc.), or when it comes to communications related to minors or vulnerable groups, which may be subject to special protection and attention by the public administrations and, as a logical consequence, holders of particularly sensitive information (art. 9 RGPD and art.

LOPD).

There are several examples of the use of SMI by public administrations and public and private entities, and it should be noted that, in many of these communications, there is no flow of particularly protected or sensitive information. In other cases,

for example, if an SMI is used for the transmission of health data to healthcare services, or for communication between a victim of an assault and the security forces, there could be an informative flow of data that the regulation especially protects. We refer, in this sense, to the considerations made in FJ VIII of Opinion 55/2016, with regard to the problems that, from the perspective of the protection of personal data, present the use of SMI in cases where it is not only predictable, but usual, that sensitive information is communicated, in which the use of certain SMIs may even be inadvisable.

However, due to the information available, the type of personal information that could be the subject of communication in the context of Groups 1, 2 and 3 (disclosure of activities, calling or cancellation of events, of the municipal toy library, of the Culture Council or the Children's Council), would not be information deserving of special protection for the purposes of data protection regulations.

Therefore, taking into account the flow of information and the purpose of the Groups that would be created by the City Council, which do not involve, according to the information available, the treatment of specially protected information, the use of a widely known and used SMI cannot be ruled out by citizens, such as Whatsapp, which the City Council specifically refers to, or other SMI with similar benefits and characteristics, although the considerations that will be made below will have to be taken into account.

VI

Having said that, the inquiry concerns the consent of the parents (in relation to Case 1, although the same doubt is raised for Cases 2 and 3), in order for their phone number to be included in the Whatsapp Group . Apart from this, the query asks what other parameters should be taken into account in order to comply with data protection regulations. Specifically, the City Council asks if it would be correct (in addition to limiting the purpose of the group to the maximum), to include a policy clause of good use by the users (citizens) of the Group, of a commitment that they will not transfer to third parties or group phones, nor the profile photo, nor even the images that can be shared in the group (the query cites as an example "that some parent will hang in the group a photo in which the attendees of the event will be identified, adults and minors".
The consultation also raises questions about the extent to which the City Council would be responsible for the comments or data that members can make in the group, and about the power to expel someone from the group, in case they do not use it responsibly. The query makes it clear that these doubts can be extended to Cases 2 and 3.

At the outset, being part of a Whatsapp Group means that all participants in the Group will have access to the contact information of the rest (name, phone number, status, photo or profile picture, if applicable...) in short, that there will be a communication of personal data between the participants in the Group, not only with regard to the messages transmitted by the City Council but also to the contact data used by Whatsapp and which are visible to the different members of a Whatsapp Group (for more details, please refer to the information available in the FAQs section of the Whatsapp website). They will also have access to the content of messages that citizens can send through this SMI.

One of the fundamental principles on which the processing of personal data is based is the principle of legality. According to Article 6 of the RGPD:

"1. The treatment will only be lawful if at least one of the following conditions is met:

a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes;

(...).”

According to article 4.11 of the RGPD, the consent of the interested party is: "any manifestation of free will, specific, informed and unequivocal by which the interested party accepts, either through a statement or a clear affirmative action, the treatment of personal data concerning you;"

The purpose of creating the Groups subject to consultation is to inform the participating people of different issues and information of interest, a purpose that, initially, can be achieved by other means. This leads to consider that the legal basis on which the participation of the affected persons in Whatsapp Groups (cases 1, 2 and 3 of the consultation) should be based should be the consent of these affected persons, who voluntarily agree to be part of it through a clear affirmative statement or action.

It is possible that the City Council has the telephone number or other personal identifying and contact information of the people who are expected to be able to participate in the Groups (parents of minors who attend the toy library, representatives of associations in the municipality and, obviously, councilors or staff of the City Council itself), for certain purposes (collection of toy library fees, management of the employment relationship of municipal workers, exercise of councillors' functions, etc.).

However, in accordance with the purpose principle, in order to process the contact data of the affected persons with the purpose of creating SMI Groups for the management of certain activities, the City Council should have the consent of all those affected , not only from people outside the City Council (citizens), as the inquiry seems to point out.

This is so because, for example, the City Council has personal data of its employees for various purposes - such as those derived from the employment relationship itself -, so that the treatment of this data by the City Council can be lawful (eg art. 6.1.b) RGPD), without the worker's consent being necessary. However, it does not seem that the membership of a municipal worker in one of the Instant Messaging Groups subject to consultation is required of the worker by the mere fact of his employment relationship with the City Council.

Therefore, the City Council should request consent (a "clear affirmative action", in the terms of Article 4.11 RGPD), not only from "citizens" (parents of minors who attend the toy library - Case 1 -, members of village associations -Case 2-, or school students -Case 3-), but also to municipal workers or councilors who, if applicable, can participate in the respective Group, consent that would need to be collected, in any of the cases, prior to the creation of the Instant Messaging Groups.

However, it must be noted that, in order for the treatment to be based on consent, it is necessary for the people participating in the Groups to have other alternative channels of communication with the City Council, for the intended purposes, that is to say, that do not impose on them as the only means of communication, having to be part of the Whatsapp Group. If this were the case, and there were no other alternative channels, it does not seem that the consent could be considered "free", in the terms of article 4.11 RGPD.

It should be added that Case 3, referring to the Whatsapp Group of the Children's Council, has the particularity that, among others, minors representing the school would be part of it. The consultation does not provide more information about the age of these minors, or about the schools that could be part of them.

It should be borne in mind that, in relation to the conditions applicable to the consent of minors, article 8 of the RGPD provides that:

> "1. When article 6, section 1, letter a) is applied, in relation to the direct offer to children of services of the information society, the treatment of the personal data of a child will be considered lawful when it has at least 16 years If the child is under 16 years of age, such treatment will only be considered lawful if consent is given or authorized by the holder of parental authority or guardianship over the child, and only to the extent that it is given or authorized. The Member States may establish by law a lower age for such purposes, provided that this is not lower than 13 years.

It should also be added that in the case of Spain there are regulations that lower this age. Thus, article 13 RLOPD, currently still in force, provides for the possibility that minors, who are over 14 years of age, can provide their own consent for the processing of their data, in the following terms:

> "1. The data of those over the age of fourteen can be processed with their consent, except in cases where the law requires the assistance of the holders of parental authority or guardianship for their provision. In the case of children under the age of fourteen, the consent of parents or guardians is required. (...)
>
> 4. It is up to the person in charge of the file or treatment to articulate the procedures that guarantee that the age of the minor and the authenticity of the consent given, if applicable, by the parents, guardians or legal representatives have been effectively verified."
>
> (...)."

In relation to this, we note that the Draft Organic Law on the Protection of Personal Data (BOCCGG, of 24.11.2017), which is in the parliamentary processing phase, provides, in its article 7, the following:

> "Article 7. Consent of minors.
>
> 1. The treatment of the personal data of a minor can only be based on his consent when he is over thirteen years old.
> The cases in which the law requires the assistance of the holders of parental authority or guardianship for the celebration of the legal act or business in whose context consent for the treatment is obtained are excepted. (...).

Given that, as has been pointed out, the lawfulness of the processing of the data of these students would be based on prior consent, the City Council will have to ask for the consent of the students themselves, in the event that they are minors over the age of 14 or, in the event that it may be minors who are not yet 14 years old, the City Council will need to obtain the consent of their parents or legal representatives. This is without prejudice to the specific conditions established by the SMI to register for the application.

In conclusion, the fact that the City Council has the consent of all the participants in Groups 1, 2 and 3, would legitimize not only the creation of the Groups, but, as a logical consequence, the access by the participants of each Group to the data of the other users of the group (phone number, photo or profile image,...), and the information they share (text messages, voice messages, photographs...), to give compliance with the specific purpose of the different Groups.

VII

Having said that, the City Council asks if it would be correct (in addition to limiting the purpose of the group as much as possible), to include a policy clause of good use by the users (citizens) of the Group, of a commitment that they will not transfer to third parties or group phones, nor the profile picture, nor even the images that can be shared in the group (the query cites as an example "that some parent will hang in the group a photo in which the attendees of the event will be identified, adults and minors").

At the outset, as has been pointed out, the creation of the SMI Groups (Cases 1, 2 and 3), have a clear and specific purpose, which the consultation itself explains. By application of the principle of purpose (art. 4.2 LOPD), and taking into account that the regulations require that the data be treated lawfully, loyally and transparently (art. 5.1.a) RGPD), it is clear that the data must be collected for specific, explicit and legitimate purposes, and which must not be subsequently treated in a manner incompatible with these purposes (art. 5.1.b) RGPD).

The City Council, as responsible and administrator of the Groups, must foresee and explain in an appropriate way to the people who will be participants, what is the purpose of the Group's communication, with as much detail as possible and in an understandable way such as, of done, points out the query itself.

We agree that the RGPD gives a letter of nature to the principle of transparency (consideration 39 and consideration 58 RGPD). According to article 5.1.a) of the RGPD, the data must be treated lawfully, loyally and transparently in relation to the interested party.

The principle of transparency, linked to the principles of legality and loyalty (art. 5.1.a) RGPD), specifically includes the duty of the person in charge to inform those affected about a series of issues, under the terms of article 13 RGPD, to which we refer, and which in some aspects goes beyond what is provided for in article 5 LOPD. Therefore, the City Council, as responsible for the processing of data of certain natural persons - for the purposes of interest, the people who can participate in the different SMI Groups created by the City Council - must inform them about the said treatment, among others, on the purpose of the same, and the legal basis of this treatment (art. 13.1.c) RGPD).

From the date of application of the RGPD, it will be necessary to report the following aspects (Article 13 RGPD): the contact details of the data protection representative; the legal basis of the treatment; the legitimate interests pursued on which the treatment is based; the intention to transfer the data to a third country or international organization and the basis for doing so; the period during which the data will be kept; the existence of the right to request portability; the right to withdraw at any time the consent that has been given; if the communication of data is a legal or contractual requirement or a necessary requirement to enter into a contract; the right to present one

complaint before a control authority; the existence of automated decisions, including the logic applied and their consequences.

Clauses that do not take into account the degree of understanding of the average citizen, but even abuse legal terminology, would not be admissible, as stated by WG29, in the document Guidelines on Consent ("Guidelines on Consent under Regulation 2016/679", of November 28, 2017): "When requesting consent, controllers must ensure that they use clear and simple language in all cases. This means that a message must be easily comprehensible to the average person and not only to lawyers. Controllers cannot use long unreadable privacy policies or statements full of legal jargon."

For the purposes of interest in this opinion, the City Council will have to put special emphasis on informing the participants in the Groups in an understandable way, and prior to the start-up of these Groups, on the one hand, about the fact that the participants in the Group they will be able to access the contact details of the other participants, and on the other hand, about the fact that the participants will be able to access the information contained in the messages (written, voice, attached files, photographs...) that communicate through the Group.

Regarding the fulfillment of the duty of information in relation to minors who may be part of the Group of the Children's Council (Case 3), we note that, according to article 13.3 RLOPD: "When the treatment is refers to the data of minors, the information addressed to them must be expressed in a language that is easily understandable to them, with express indication of the provisions of this article." According to Recital 58 of the RGPD "(...). Given that children deserve specific protection, any information and communication whose treatment affects them must be provided in a clear and simple language that is easy to understand."

Therefore, in relation to minors who can give consent on their own behalf (minors over the age of 14, notwithstanding the provisions that may be contained in the Draft Organic Data Protection Law, to which we have referred, which is in its parliamentary seat), the information provided to them must be specially adapted to their level of understanding.

VIII

The query asks about the responsibility that the City Council could have regarding the assignment that the participants of the Groups can make to third parties. It is worth saying that the query refers, at this point, to parents or citizens who participate in the Groups.

In any case, as a preliminary matter, it is appropriate to distinguish the processing of data by councilors or employees of the City Council itself who are part of the Groups, from the processing that can be done by citizens (parents, students, or members of associations), who they do not, in principle, and according to the information available, have any employment or organic link with the Consistory.

As this Authority has agreed in previous Opinions, it must be borne in mind that if the councilors' access to personal data occurs due to the functions entrusted to them as such (as could be the case, according to the information available, of the councilors referred to in the query), these must be governed by the reserve duty imposed by the local regulations (article 164.6 of the Text of the Municipal and

local regime of Catalonia, approved by Legislative Decree 2/2003, of April 28 (TRLMRLC), according to which "the members of the corporation must respect the information to which they have access by reason of the position if the fact of publishing -it may harm the interests of the local body or third parties").

Apart from this specific provision that would affect the councillors, the municipal workers who, according to the consultation, could be part of the Groups, are bound by the duty of confidentiality imposed on them by the regulations as public workers (art. 52 of the Statute basic of the public worker, approved by Royal Legislative Decree 5/2015, of October 30 (EBEP)), as well as the general duty of secrecy imposed by article 10 LOPD, according to which: "The person responsible for the file and those who intervene at any stage of the processing of personal data are obliged to professional secrecy with regard to the data and the duty to save them, obligations that remain even after the end of their relationship with the owner of the file or, if where appropriate, with their manager".

In addition, according to the provisions of the Penal Code (articles 197 and 198), the authority or public official who, outside of the cases permitted by law and prevailing in his position, disseminates, reveals or transfers certain data to third parties, would be carrying out a conduct that could be constitutive of the crime of discovery and disclosure of secrets.

This, together with the requirement derived from the principle of purpose, means that councilors and City Council workers who, by reason of their position, may be part of the Groups subject to consultation, in the event of disclosure to third parties, or treat the information (whether contact details of other members of the Group, or other personal information), without the consent of those affected and for other purposes other than the Group's own, could contravene the regulations for the protection of personal data.
Disciplinary liability may even arise in certain cases (art. 83 RGPD and art. 46.2 LOPD).

Therefore, the City Council could be held responsible for inappropriate treatment that, for example, is carried out by a municipal worker who is part of the Group and who intervenes because of his position.

Regarding parents of children who go to the toy library, members of village associations or minors in schools, even though the creation of Groups 1, 2 and 3, is at the initiative of the City Council , it would hardly be directly responsible (for the purposes of Article 46 LOPD) for the subsequent use of personal data (comments, contact numbers, photos...) by persons outside the City Council, to which they will have accessed legitimately, in the terms indicated.

Having said that, it should be borne in mind that, in principle, any person who accesses the personal data of others for a legitimate purpose, should treat the personal data to which they have been able to access in accordance with the principles and guarantees of the regulations for the protection of data, quotes

Thus, in principle, citizens who participate in the Groups should treat the personal data to which they have access within the framework of the Group's own purpose. The members of the Group should have the consent or other legal authorization to communicate to persons outside the same, the personal information it deals with. The general duty of secrecy (art. 5.1.f) RGPD and art. 10 LOPD) would also apply in this case. By way of example, to communicate the telephone number of another member of the Group to a third party unrelated to him, his consent would be required.

In the specific case of the image of people, which is personal data (art. 5.1.f) RLOPD), as this Authority has done on previous occasions (Opinions CNS 9/2016, or CNS 64/2015, among others), the capture and dissemination of the graphic image of identified or identifiable persons affects the right to image (art. 18.1 EC) and, therefore, it is necessary to take into account Organic Law 1/1982, of May 5, on civil protection of the right to honor, personal and family privacy and one's image (LO 1/1982). The provisions of LO 1/1982 (arts. 7.5 and 8.2), could enable the capture and dissemination of images of identifiable people (for example, through photographs) in a public event and in which the image of these people appears as a mere accessory.
If so, it would not be strictly necessary, from the point of view of the regulations studied, to have the prior consent of those affected, so that the members of the Groups could transfer such images to third parties. On the other hand, in other types of images in which these elements are not given, it would be necessary to have the consent of those affected.

In any case, and without prejudice to this clarification, it would not be contrary to data protection regulations and, even, it could be advisable for the City Council to establish, as a policy of good use, that the members of the Groups do not share images with third parties outside the Group, unless they have the consents that may be necessary, given the aforementioned regulations.

Leaving aside the photographs, and with reference to other types of information that can be shared in the Groups, it is advisable for the City Council to warn the participants of the Groups to share with third parties specially protected information (such as health data , a possibility indicated by the query) could contravene the provisions of the personal data protection regulations. At this point, for illustrative purposes, and due to its relevance, we refer to the Judgment B. Lindqvist, of the Court of Justice of the EU, of November 6, 2003. This, without prejudice to the fact that, for the information of what is available, it does not appear that the purpose of Groups 1, 2 and 3 makes the processing of specially protected information likely.

For all that has been said, given the problems raised by the consultation (possible dissemination of photographs, comments, etc., by the participants), it is necessary to positively assess that the City Council draw up a "good use policy clause" (a code of good practices, in short), so that all participants in the Groups (regardless of whether or not they are linked to the City Council) treat the personal data subject to consultation in accordance with the provisions of the aforementioned regulations.

Finally, with regard to the possibility of expelling a member of the Group, to which the query refers, from the perspective of data protection it is not up to this Authority to determine in which cases the City Council must take the decision expel a member from any of Groups 1, 2 and 3.

However, the mere fact of having expelled a member of the SMI Group does not detract from the City Council's obligation to comply with the principles and obligations, in terms of data protection, that may correspond to it as responsible, nor nor the consequences that inadequate processing of personal data may entail.

IX

Case 4 refers to a Whatsapp Group that, according to the information available, was not created by the City Council, but by "the young people of the town", although, according to the query, it would have been added to this Group a municipal worker, using a number

telephone number of the City Hall itself. The City Council asks if, as it is not an administrator of the Group, the City Council would have any responsibility as an Administration, and if it should carry out any management with reference to the LOPD.

Given the information available, it must be assumed that the purpose of the Group in question is unknown, that is, if it could have any relationship, direct or indirect, with any activity or service provided or organized by the City Council. It is not known whether certain personal information for which the City Council is responsible could be processed within the framework of this Group. It is also unknown whether the municipal employee who, according to the consultation, would have been added to the Group, would be part of it in his capacity as a City Council employee and by reason of his work, or in a private capacity.

In relation to this issue, the RGPD provides that this Regulation does not apply to the processing of personal data carried out by a natural person in the exercise of exclusively personal or domestic activities (Recital 18 and art. 2.2.c) RGPD). The exclusion that was already contained in the LOPD regarding treatments carried out by natural persons in the exercise of exclusively personal or domestic activities (art. 2.2.a) LOPD), understanding as such those that fall within the framework of the private or family life of individuals (art. 4.a) RLOPD) or, as specified by the National Court in the Judgment of June 15, 2006: "(...) It will be personal when the data processed affect the the most intimate sphere of the person, to their family and friendship relationships and that the purpose of the treatment is nothing other than to produce effects in those areas."

Therefore, given the information available, this Authority cannot determine whether the Group referred to (Case 4) has an exclusively personal or domestic purpose and, consequently, whether the data processing that may be carried out there is or not subject to personal data protection regulations.

On the other hand, from the information provided, it seems clear that this would not be a treatment that is the responsibility of the City Council, regardless of whether a certain employee of the corporation has been added to it in a private capacity.

In any case, the worker, given his employment relationship with the City Council, has the obligation to treat the personal information of which he may be aware by reason of his position, with full respect for the principles and guarantees of the regulations for the protection of data, given the aforementioned regulations.

In accordance with the considerations made in this opinion, the following are made,

Conclusions

When establishing the use of a certain communication channel in municipal services, the City Council must take into account the guarantees offered by the channel for the treatment of the information of the affected persons and the existence or not from other alternative channels.

Cases 1, 2 and 3: The City Council must comply with the principles and guarantees of the data protection regulations, among others, it must have the consent of all the participants of the Groups, unless it has another basis legal and give them information about the processing of data (art. 13 RGPD) and the consequences that may arise from the use of this channel.

Although the creation of the Groups is at the initiative of the City Council, it would hardly be directly responsible (for the purposes of Article 46 LOPD) for the subsequent use of personal data by persons outside the City Council. Without prejudice to this, the development of a "good use policy clause" is positively valued, so that all participants in the Groups treat personal data in accordance with the provisions of the regulations.

Case 4: Given the information available, it cannot be determined whether the Group has an exclusively personal or domestic purpose and, consequently, whether or not it is subject to personal data protection regulations. In any case, for the information provided, it would not be the responsibility of the City Council.

Barcelona, April 26, 2018