CNS 13/2018

Dictamen en relació amb la consulta d'un Ajuntament sobre l'ús de Whatsapp per part d'una administració local

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un Ajuntament, en el que planteja diverses qüestions respecte els riscos i responsabilitats que suposa l'ús de l'aplicatiu de Whatsapp per a determinades finalitats en el context d'una administració local.

La consulta planteja el grau d'adequació a la normativa de protecció de dades en relació amb diferents casos en què s'estaria plantejant la possibilitat d'utilitzar Whatsapp. Aquests casos es refereixen a la comunicació amb els pares de menors usuaris de la ludoteca municipal; amb la comunicació entre membres del Consell municipal de Cultura (regidors, membres d'associacions del municipi...); amb la comunicació entre membres del Consell de la Infància (regidors, menors d'edat representants de l'escola...); així com en relació amb un grup de Whatsapp que hauria creat un grup de joves del poble.

La consulta pregunta, entre d'altres aspectes, respecte la responsabilitat que podria tenir l'Ajuntament en relació amb la utilització d'aquest canal de comunicació, o respecte el consentiment que caldria demanar als participants del grup.

Analitzada la petició, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

L'Ajuntament pregunta sobre el grau d'adequació a la normativa de protecció de dades en relació amb diferents casos en què, segons la consulta, l'Ajuntament estaria plantejant la possibilitat d'utilitzar Whatsapp, en concret, en els supòsits següents:

Cas 1: Grup de Whatsapp municipal en què s'inclouria els pares de nens usuaris de la ludoteca municipal, l'administrador del qual seria un treballador municipal que utilitzaria un telèfon de propietat municipal. Segons la consulta, la finalitat és la divulgació d'actes que es realitzen a la ludoteca, modificacions d'horaris, cancel·lacions d'actes, etc.

Cas 2: Grup de Whatsapp del Consell de Cultura, els integrants del qual serien els seus membres (regidors, membres d'associacions del poble...) i personal municipal, i l'administrador del Grup seria l'Ajuntament. La finalitat seria, segons la consulta, l'enviament de convocatòries, cancel·lacions, etc.

Cas 3: Grup de Whatsapp del Consell d'Infància, els integrants en serien els membres del Consell (regidors, menors d'edat representants de l'escola...) i personal municipal, i l'administrador del Grup seria l'Ajuntament. La finalitat del qual seria, segons la

consulta, l'enviament de convocatòries, cancel·lacions, etc. En aquest cas, la consulta remarca la peculiaritat que s'inclouria a menors d'edat en el grup.

Pel que fa als casos 1, 2 i 3, l'Ajuntament planteja els mateixos dubtes, referits, en síntesi, al consentiment de les persones participants en els grups, o a la responsabilitat de l'Ajuntament respecte els comentaris o dades que els participants poguessin difondre.

Cas 4: Grup de Whatsapp que, segons la consulta, haurien creat joves del poble. La consulta no aporta informació sobre la finalitat del Grup. La consulta puntualitza que l'Ajuntament no és l'administrador del Grup, i que s'hi hauria afegit un treballador municipal utilitzant un número de telèfon del propi Ajuntament. La consulta planteja si, en no ser administrador del grup, l'Ajuntament tindria alguna responsabilitat com a Administració pública, i si hauria de realitzar alguna gestió en relació amb l'LOPD (Llei orgànica 15/1999, de 13 de gener, de protecció de dades de caràcter personal).

Situada la consulta en aquests termes, ens referirem de forma conjunta als Casos 1, 2 i 3 que planteja l'Ajuntament, ja que són substancialment coincidents pel que fa a les seves característiques (són Grups creats pel propi Ajuntament per comunicar informació sobre serveis o activitats municipals) i pel que fa als dubtes que plantegen; de forma separada es farà referència al Cas 4, citat.

III

A mode d'introducció, cal fer notar que els mitjans o serveis de comunicació que poden utilitzar les administracions públiques (en aquest cas, un Ajuntament), ja sigui per relacionar-se amb els ciutadans o amb altres administracions públiques, o com a canal de comunicació intern dins la seva pròpia estructura, poden ser molts i de naturalesa molt variada (mitjans de comunicació tradicionals (premsa, ràdio o televisió), Internet, webs pròpies dels organismes i ens públics, Intranets corporatives, correu ordinari, comunicació per via telefònica, comunicació presencial, etc.

En la mesura que l'ús de qualsevol mitjà, canal o servei de comunicació per part de l'Ajuntament comporti un tractament d'informació personal, aquest tractament haurà de sotmetre's als principis i garanties de la protecció de dades, és a dir, l'RGPD, que va entrar en vigor el 25 de maig de 2016, i que serà aplicable a partir del 25 de maig de 2018 (art. 99 RGPD). També cal tenir en compte, fins a la plena entrada en vigor de l'RGPD en la data indicada, les previsions de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), i el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de l'LOPD (RLOPD).

Des del moment que l'Ajuntament habiliti un canal de comunicació amb els ciutadans i/o els seus treballadors o regidors, el tractament de dades dels afectats o interessats (art. 4.1 RGPD i art. 3.e) LOPD) que se'n derivi haurà d'estar sotmès als principis i garanties de la normativa de protecció de dades, en els termes de la normativa esmentada.

En concret, l'Ajuntament es refereix a la utilització del sistema de missatgeria instantània (SMI) de Whatsapp. Els SMI són canals de comunicació en temps real entre dues o més persones, basada principalment en text, que s'envia a través de dispositius connectats a una xarxa com ara Internet. Aquestes apps, com la de Whatsapp, o similars, permeten adjuntar missatges de text, i arxius d'imatges, vídeo i

àudio, és a dir, altres continguts a banda del propi missatge de text. A més d'utilitzar la missatgeria bàsica, els usuaris d'aquests sistemes poden fer videoconferències, crear grups més o menys nombrosos (com seria el cas dels Grups als que es refereix la consulta), "xats", i compartir-hi informació, arxius o contactes.

En qualsevol cas, és clar que el fet de crear un Grup de Whatsapp -o, per extensió, d'altres SMI similars, dels moltes disponibles actualment en el mercat-, implica un tractament de dades de caràcter personal. D'una banda, les dades personals identificatives dels membres del Grup (noms, pseudònims utilitzats, número de mòbil, fotografia de perfil, etc), i de l'altra, la informació personal que es pugui contenir en els missatges que es trameten, ja siguin per escrit, missatges de veu, imatges, etc.

Des del moment que aquesta informació es refereix a persones físiques, es tracta d'informació personal sotmesa a la protecció de la normativa corresponent (LOPD i RLOPD, fins el 25 de maig de 2018, i RGPD, a partir del 25 de maig de 2018).

El Parlament de Catalunya ha dictat la Resolució 280/XI, del Parlament de Catalunya (BOPC 220, de 27 de setembre de 2016), sobre l'ús de serveis de comunicacions pel Govern, segons la qual s'insta el Govern a fomentar l'ús de SMI, per part de les Administracions públiques, que tinguin determinades característiques, entre d'altres, una política de privacitat d'acord amb la legislació vigent en matèria de protecció de dades, que practiquin la transparència, i que incorporin les mesures que estableix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, del 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, d'acord amb els terminis establerts.

Fem avinent que aquesta Autoritat ha analitzat la utilització de SMI des de la perspectiva de la protecció de dades en ocasions anteriors així com, específicament, el contingut de la Resolució 280/XI, citada (Dictàmens CNS 24/2013, CNS 55/2016, o CNS 54/2017, als que ens remetem).

IV

Segons l'article 4.7 RGPD (i art. 3.b) LOPD), és responsable del tractament*: "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;"*

El responsable del fitxer o tractament és qui, en primera instància, està obligat a donar compliment als principis i garanties de la protecció de dades personals.

Quan una Administració pública, com ara un Ajuntament, ha de tractar informació personal dels afectats per al compliment de les seves funcions i competències, aquesta administració és la primera responsable dels fitxers o del tractament de dades que duu a terme. Així, quan l'Ajuntament exerceix les seves funcions en relació, amb la gestió d'espais municipals (com ara una ludoteca), o en relació amb competències municipals en l'àmbit de la cultura o d'infància, entre d'altres, el tractament de dades que es genera en compliment d'aquestes competències municipals, comporta que l'Ajuntament hagi de vetllar pel compliment de la normativa de protecció de dades.

Per tant, l'Ajuntament serà responsable de la informació personal que tracti a través de qualsevol SMI o que reculli per aquesta via.

Al marge d'això, la utilització de SMI per part de les Administracions públiques, presenta una singularitat, atès que és el propi usuari (la persona física), qui decideix instal·lar-se una determinada aplicació de missatgeria instantània, a través de la qual es pot relacionar amb tercers, incloses, si escau, les Administracions públiques.

Com ha fet avinent aquesta Autoritat, les empreses titulars dels SMI (com ara Whatsapp), decideixen quin tractament fan de les dades dels usuaris que decideixen utilitzar el seu servei de missatgeria, i les que estableixen les condicions d'ús corresponents. En la informació que, habitualment, es posa a disposició dels usuaris a través dels respectius llocs web (als efectes que interessen, www.whatsapp.com), aquestes empreses determinen quina informació utilitzaran i quina no, incloent dades personals de l'usuari i dels contactes de l'usuari, i per a quines finalitats.

A partir d'aquí, qualsevol empresa de SMI que tracti dades dels seus usuaris, també haurà de donar compliment als principis i garanties de la normativa de protecció de dades, en els termes que correspongui.

Certament, és l'empresa responsable del SMI la que ha de garantir que compleix la normativa de protecció de dades, però aquesta és una qüestió que també ha de tenir present l'Ajuntament a l'hora de decidir prestar els seus serveis a través d'un determinat canal de comunicació. L'Ajuntament ha d'assegurar-se que el canal de comunicació s'ajusta a les exigències de la normativa.

L'Ajuntament, és responsable de tractar dades personals en relació amb l'ús de la ludoteca, o en relació amb l'activitat dels Consells de Cultura o d'Infància, entre d'altres, i com a tal és responsable de la informació personal que recull dels propis afectats (pares de la ludoteca, representants veïnals, alumnes d'escola, o dels seus propis regidors i treballadors municipals), i del tractament posterior que se'n faci.

Als efectes que interessen, des del moment que l'Ajuntament valora la possibilitat crear un Grup o un xat de SMI (Whatsapp, o d'altres similars) per comunicar-se amb els afectats que integraran el Grup (ciutadans, regidors, treballadors municipals, etc), i gestionar així determinada activitat o servei municipal, haurà de tenir en compte que això generarà un flux informatiu (de dades identificatives i de contacte de la resta de membres de cada Grup, i de la informació que es comparteixi en el Grup, com ara missatges de text o de so, imatges...), entre els participants, que s'ha d'ajustar a les exigències de la normativa de protecció de dades.

En aquest sentit, fem avinent que hi ha una diferència substancial entre les diferents comunicacions que pot establir l'Ajuntament, en el cas que ens ocupa.

D'una banda, res impedeix que l'Ajuntament tracti les dades de les que disposa com a responsable (per exemple, dels pares de la ludoteca), per establir-hi una comunicació de forma directa i bidireccional, per al compliment de finalitats legítimes; en aquest cas no hi ha accés de tercers a la informació que es pugui compartir entre l'Ajuntament i l'afectat.

Ara bé, si l'Ajuntament, com a responsable de les dades personals dels afectats, tracta les dades de contacte per crear una llista de participants per crear un Grup de SMI, haurà de tenir una base legal adequada per dur a terme aquest tractament, tenint en compte que en aquest cas el flux informatiu es multiplica, ja que tant les dades de

contacte com el contingut dels missatges, estaran a l'abast de tots els participants en el Grup.

Això obliga a l'Ajuntament, a l'hora de crear Grups de SMI, a ser especialment curós i a analitzar una sèrie de qüestions, com ara la base legal del tractament, i la informació que haurà de donar als membres del Grup, per tal que el flux informatiu esmentat (entre tots els participants del Grup) s'ajusti a les exigències de la normativa de protecció de dades.

Feta aquesta consideració general, cal dir que Whatsapp, al que es refereix la consulta, és una empresa radicada fora de la Unió Europea. Ara bé, segons disposa l'article 2.2 de l'RGPD:

> *"2.El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:*
> *a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o*
> *(...)."*

Per tant, quan Whatsapp s'utilitza en dispositius d'usuaris que, com en el cas que ens ocupa, es troben a Espanya, és indubitada l'aplicació dels principis i garanties de la normativa de protecció de dades personals (LOPD, RLOPD, i RGPD) als casos objecte de consulta.

Aquesta Autoritat ha posat de manifest en ocasions anteriors diverses problemàtiques que presenta el tractament de dades per algunes empreses de missatgeria instantània, entre d'altres -tot i que no exclusivament-, Whatsapp, des de la perspectiva de la protecció de dades.

Són diverses les actuacions dutes a terme en els darrers anys per autoritats europees de protecció de dades en relació amb el tractament de dades d'usuaris a la UE per part de Whatsapp, com ara els informes i investigacions de diverses Autoritats de protecció de dades (Autoritat de Protecció de Dades d'Holanda i Autoritat federal de Canadà, de gener de 2013). També cal recordar la intervenció del GT 29, a través de diversos escrits adreçats a Facebook i Whatsapp (27 d'octubre de 2016, 16 de desembre de 2016 i 24 d'octubre de 2017), en què s'han posat de manifest diverses deficiències en el mecanisme de prestació del consentiment dels usuaris arran de la previsió de comunicació de dades a Facebook, ("*Facebook family of companies*"), per un conjunt de finalitats que inclouen el màrqueting i la publicitat.

Entre d'altres qüestions, cal tenir en compte el principi de consentiment (art. 4 LOPD i art. 4.11 RGPD). És notori que diverses empreses de SMI, entre d'altres, Whatsapp, inclouen condicions generals o estàndards, fixades i modificades unilateralment per l'empresa, sense deixar marge d'opció a l'usuari. Tot i que pot ser raonable que l'usuari hagi d'acceptar necessàriament un cert nivell de tractament de les seves dades en la mesura que això pugui ser necessari des d'un punt de vista tècnic per a la prestació del servei de missatgeria, això no implica que resulti adequada la prestació d'un consentiment general i, podríem dir, "indiscriminat", en el sentit d'una acceptació incondicionada, per utilitzar les dades de l'usuari o de terceres persones per a finalitats que no resulten estrictament necessàries per a la prestació del servei.

En aquest sentit, l'RGPD (Considerants 32 i 43) estableix la rellevància de la granularitat en la prestació del consentiment, element que no resulta nou en l'àmbit

que ens ocupa, doncs ja havia estat expressament citat i recomanat pel GT 29, en el seu Dictamen 2/2013, sobre apps en dispositius intel·ligents ("*Opinion 2/2013, on apps on smart devices*"), de 27 de febrer de 2013, i reiterat pel GT 29 en el document *"Guidelines on Consent under Regulation 2016/679",* de 28 de novembre de 2017.

Com es desprèn de la informació disponible al web de Whatsapp ("*Términos de Servicio de Whatsapp*"): *"Libreta de direcciones. Nos proporcionas regularmente los números de teléfono de los usuarios de Whatsapp y los demás contactos que tienes en la libreta de direcciones de tu teléfono móvil."* (...), es pot apuntar que Whatsapp no aplica un consentiment granular que permeti l'usuari seleccionar els contactes a què tindrà accés.

D'altra banda, com es desprèn de les consideracions i advertiments provinents de les Autoritats de protecció de dades europees en els darrers anys i, més recentment, de la Resolució R/00259/2018, de l'Agència Espanyola de Protecció de Dades, en què es sanciona a Whatsapp per cedir a Facebook dades personals sense el consentiment adequat dels afectats, Whatsapp no aplicaria el consentiment parcel·lat en relació amb les cessions de dades dels usuaris a tercers, i no hauria permès als afectats excloure determinada informació personal de les dites cessions a Facebook, que a tenor de les recents opinions i resolucions de diverses Autoritats de protecció de dades, serien cessions clarament innecessàries i, per tant, haurien hagut d'estar subjectes al consentiment dels usuaris.

També cal tenir en compte que l'RGPD dona carta de naturalesa al principi de transparència (considerant 39 i considerant 58 RGPD). Segons disposa l'article 5.1.a) de l'RGPD, les dades han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat. El principi de transparència, vinculat en l'RGPD als principis de licitud i de lleialtat, engloba específicament el dret d'informar els afectats sobre una sèrie de qüestions, en els termes de l'article 13 RGPD (que en alguns aspectes va més enllà del que disposa l'article 5 LOPD), que recull la informació que el responsable, en aquest cas l'empresa responsable d'un SMI, en aquest cas, Whatsapp, hauria de donar a l'afectat, també de manera granular i per capes ("*layered and granular information"*). Com ha fet avinent aquesta Autoritat, no només Whatsapp, sinó també altres SMI d'utilització força habitual, podrien presentar mancances pel que fa al compliment de les exigències de l'article 13 RGPD, en definitiva, de la informació que proporcionen als seus usuaris.

Finalment, la tercera consideració que, sense ànim d'exhaustivitat, caldria tenir en compte respecte el tractament de les dades dels usuaris per part de Whatsapp (a la que específicament es refereix la consulta i a la que, per tant, ens referim), es situa en l'àmbit de la seguretat aplicable.

Entre d'altres qüestions, com ha fet avinent aquesta Autoritat (FJ VIII Dictamen CNS 24/2013; FJ X Dictamen CNS 55/2016), les previsions que puguin explicitar les empreses responsables (en aquest cas, Whatsapp), respecte la confidencialitat amb la que tracten les dades dels usuaris (mesures d'encriptació de la informació, etc), són especialment rellevants. En qualsevol cas, fem notar que l'RGPD, aplicable a partir del 25 de maig de 2018, configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt (segons l'esquema de la LOPD i RLOPD), sinó en determinar, arran d'una prèvia valoració dels riscos, quines mesures de seguretat són necessàries en cada cas, tenint en compte el tipus d'informació tractada (Considerant 83, i arts. 24.1 i 32.1 RGPD). En l'article *"WhatsApp rolls out end-to-end encryption to its over one billion users",* de l'Organització EFF, disponible en traducció al castellà: https://www.eff.org/es/deeplinks/2016/04/whatsapp-estrena-cifrado-de-fin-fin-para mas-

de-un-billon-de-usuarios), s'analitza el sistema de xifratge de Whatsapp, que es qualifica com un sistema fort.

Per la informació disponible (inclòs el seu web), Whatsapp incorpora el xifratge d'extrem a extrem, de manera que només l'emissor i el receptor (i no Whatsapp) poden llegir el missatge. Aquest tipus de xifratge estaria activat per defecte per a tots els usuaris que utilitzen les darreres versions de l'app, i no es podria deshabilitar. Ara bé, segons altra informació disponible, si bé el xifratge d'extrem a extrem de Whatsapp ofereix garanties, també es detecten certes mancances que podrien portar a que aquestes mesures no fossin prou operatives. En concret, l'informe d'Amnistia Internacional (AI): *"For your eyes only?. Ranking 11 technology companyies on encryption and human rights"* (https://www.amnesty.org/download/Documents/POL4049852016ENGLISH.PDF), hauria detectat que Whatsapp no informa els usuaris que, si es fan còpies de seguretat al núvol, aquesta informació no estaria xifrada. En definitiva, existeixen vulnerabilitats detectades –no només en Whatsapp sinó en d'altres SMI disponibles al mercat-, que haurien de tenir en compte, no només els propis usuaris que s'instal·len apps de missatgeria instantània, sinó, lògicament, las Administracions públiques que en volen fer ús.

Per tot l'exposat, i sens perjudici d'algunes mancances, des de la perspectiva de la protecció de dades, en relació amb els principis de protecció de dades i la problemàtica específica que pot representar un determinat SMI (en aquest cas, Whatsapp) en relació amb el tractament de dades dels usuaris d'aquests SMI, que les Administracions han de tenir en compte, en el cas objecte de consulta resulta clau contextualitzar la possibilitat de crear i utilitzar els Grups de Whatsapp en els supòsits plantejats, en atenció al tipus d'informació que, presumiblement, i atesa la informació disponible, es podria tractar, i a la finalitat prevista.

V

Quan un Ajuntament, com a responsable (art. 4.7 RGPD), vol emprar un SMI per a les seves comunicacions amb els ciutadans, ha de tenir en compte, d'entrada, quin tipus de comunicació vol establir, en relació amb quin servei o prestació, a quines persones o col·lectius va adreçada la informació o el servei en qüestió, quin tipus d'informació es veurà afectada, etc.

Des de la perspectiva de la protecció de dades no té les mateixes implicacions utilitzar canals de comunicació amb els ciutadans amb la finalitat de donar informació o rebre consultes sobre qüestions diverses (informació sobre l'estat del trànsit, o sobre determinats serveis municipals, sobre activitats lúdiques o culturals, etc...), que implica un flux d'informació que podríem qualificar com de general o "innòcua", que la utilització dels SMI per comunicar un possible fet delictiu, un accident (comunicacions a cossos policials, a serveis sanitaris, ambulàncies, serveis a persones dependents que requereixen atenció domiciliària, etc), o quan es tracta de comunicacions relacionades amb persones menors d'edat o col·lectius vulnerables, els quals poden ser objecte d'especial protecció i atenció per part de les administracions públiques i, en lògica conseqüència, titulars d'informació especialment sensible (art. 9 RGPD i art. LOPD).

Són diversos els exemples d'utilització d'SMI per part d'Administracions públiques i d'entitats públiques i privades, i cal apuntar que, en moltes d'aquestes comunicacions, no es dóna un flux d'informació especialment protegida o sensible. En d'altres casos,

per exemple, si s'empra un SMI per a la transmissió de dades de salut a serveis assistencials, o per la comunicació entre una víctima d'una agressió i els cossos de seguretat, sí podria donar-se un flux informatiu de dades que la normativa protegeix especialment. Ens remetem, en aquest sentit, a les consideracions fetes en el FJ VIII del Dictamen 55/2016, pel que fa a la problemàtica que, des de la perspectiva de la protecció de dades personals, presenta la utilització de SMI en casos en que és no només previsible, sinó habitual, que es comuniqui informació sensible, en els quals pot ser fins i tot desaconsellable la utilització de determinats SMI.

Ara bé, per la informació disponible, el tipus d'informació personal que podria ser objecte de comunicació en el context dels Grups 1, 2 i 3 (divulgació d'activitats, convocatòria o cancel·lació d'actes, de la ludoteca municipal, del Consell de Cultura o del Consell d'Infància), no seria informació mereixedora d'especial protecció als efectes de la normativa de protecció de dades.

Per tant, tenint en compte el flux informatiu i la finalitat dels Grups que crearia l'Ajuntament, que no comporten, per la informació disponible, tractament d'informació especialment protegida, no es pot descartar la utilització d'un SMI àmpliament conegut i utilitzat per la ciutadania, com podria ser Whatsapp, al que es refereix específicament l'Ajuntament, o d'altres SMI de prestacions i característiques similars, tot i que caldrà tenir en compte les consideracions que es faran tot seguit.

VI

Dit això, la consulta es refereix al consentiment dels pares (en relació amb el Cas 1, tot i que es planteja el mateix dubte per als Casos 2 i 3), per tal que el seu número de telèfon sigui inclòs en el Grup de Whatsapp. A banda d'això, la consulta pregunta quins altres paràmetres caldria tenir en compte per tal de donar compliment a la normativa de protecció de dades. En concret, l'Ajuntament pregunta si seria correcte (a més d'acotar al màxim la finalitat del grup), incloure una clàusula de polítiques de bon ús per part dels usuaris (ciutadans) del Grup, de compromís que no cediran a tercers ni telèfons del grup, ni la fotografia del perfil, ni tan sols les imatges que es puguin compartir en el grup (la consulta cita com a *exemple "que algun padre colgara en el grupo una foto en el que se identificara a los assistentes al evento, adultos y menores".* La consulta també exposa el dubte de fins a quin punt l'Ajuntament seria responsable dels comentaris o dades que els membres puguin fer al grup, i sobre la potestat d'expulsar a algú del grup, en cas que no en fes un ús responsable. La consulta explicita que aquests dubtes són extensibles als Casos 2 i 3.

D'entrada, formar part d'un Grup de Whatsapp suposa que tots els participants en el Grup tindran accés a la informació de contacte de la resta (nom, número de telèfon, estat, foto o imatge de perfil, si escau...) en definitiva, que hi haurà una comunicació de dades personals entre els participants en el Grup, no només pel que fa als missatges transmesos per l'Ajuntament sinó també a les dades de contacte que utilitza Whatsapp i que són visibles per als diferents membres d'un Grup de Whatsapp (ens remetem, per a major detall, a les informacions disponibles a l'apartat FAQs del web de Whatsapp). També tindran accés al contingut dels missatges que puguin enviar els ciutadans a través d'aquest SMI.

Un dels principis fonamentals en què es basa el tractament de dades personals és el principi de licitud. Segons disposa l'article 6 de l'RGPD:

> *"1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

(...).”

Segons l'article 4.11 de l'RGPD, el consentiment de l'interessat és: *“toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;”*

La finalitat del crear els Grups objecte de consulta, és la d'informar les persones participants de diferents qüestions i informacions d'interès, finalitat que, d'entrada, es pot assolir per altres mitjans. Això porta a considerar que la base legal sobre la que hauria de fonamentar-se la participació de les persones afectades en els Grups de Whatsapp (casos 1, 2 i 3 de la consulta), hauria de ser el consentiment d'aquestes persones afectades, que voluntàriament accedeixin a formar-ne part mitjançant una declaració o acció afirmativa clara.

Pot ser que l'Ajuntament disposi del telèfon o altres dades personals identificatives i de contacte de les persones que es preveu que puguin participar en els Grups (pares de menors que assisteixen a la ludoteca, representants d'associacions del municipi i, òbviament, dels regidors o personal del propi Ajuntament), per a determinades finalitats (cobrament de quotes de la ludoteca, gestió de la relació laboral dels treballadors municipals, exercici de les funcions dels regidors, etc).

Ara bé, en atenció al principi de finalitat, per tal de tractar les dades de contacte de les persones afectades amb la finalitat de crear Grups de SMI per a la gestió de determinades activitats, l'Ajuntament hauria de disposar del consentiment de tots els afectats, no només de les persones externes a l'Ajuntament (ciutadans), com sembla apuntar la consulta.

Això és així perquè, per exemple, l'Ajuntament disposa de dades personals dels seus treballadors per a diverses finalitats –com les derivades de la pròpia relació laboral-, de manera que el tractament d'aquestes dades per part de l'Ajuntament pot ser lícita (ex. art. 6.1.b) RGPD), sense que sigui necessari el consentiment del treballador. Ara bé, no sembla que la pertinença d'un treballador municipal a un dels Grups de missatgeria instantània objecte de consulta resulti exigible al treballador pel mer fet de la seva vinculació laboral amb l'Ajuntament.

Per tant, l'Ajuntament hauria de sol·licitar el consentiment (una “clara acció afirmativa”, en els termes de l'article 4.11 RGPD), no només als “ciutadans” (pares dels menors que assisteixen a la ludoteca -Cas 1-, membres d'associacions del poble –Cas 2-, o alumnes d'escola-Cas 3-), sinó també als treballadors municipals o regidors que, si escau, puguin participar en el respectiu Grup, consentiment que caldria recollir, en qualsevol dels casos, de forma prèvia a la creació dels Grups de missatgeria instantània.

Ara bé, cal fer avinent que, per tal que la base del tractament sigui el consentiment, és necessari que les persones participants en els Grups tinguin altres canals alternatius de comunicació amb l'Ajuntament, per a les finalitats previstes, és a dir, que no se'ls imposi com a única via de comunicació, l'haver de formar part del Grup de Whatsapp. Si fos així, i no existissin altres canals alternatius, no sembla que el consentiment pugui ser considerat com “lliure”, en els termes de l'article 4.11 RGPD.

Cal afegir que el Cas 3, referit al Grup de Whatsapp del Consell d'Infància, presenta la particularitat que en formarien part, entre d'altres, menors d'edat representants de l'escola. La consulta no aporta més informació sobre l'edat d'aquests menors, o sobre els centres escolars que en podrien formar part.

Cal tenir en compte que, en relació amb les condicions aplicables al consentiment dels menors, l'article 8 del RGPD disposa que:

> *"1.Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.*

També cal afegir, que en el cas d'Espanya existeix normativa que rebaixa aquesta edat. Així, l'article 13 RLOPD, de moment encara vigent, preveu la possibilitat que els menors d'edat, que siguin majors de 14 anys, puguin prestar per ells mateixos el consentiment per al tractament de les seves dades, en els següents termes:

> *"1. Es pot procedir al tractament de les dades dels més grans de catorze anys amb el seu consentiment, excepte en els casos en què la Llei exigeixi per a la seva prestació l'assistència dels titulars de la pàtria potestat o tutela. En el cas dels menors de catorze anys es requereix el consentiment dels pares o tutors.*
> *(...)*
> *4. Correspon al responsable del fitxer o tractament articular els procediments que garanteixin que s'ha comprovat de manera efectiva l'edat del menor i l'autenticitat del consentiment prestat, si s'escau, pels pares, tutors o representants legals."*
>
> *(...)."*

En relació amb això, fem avinent que el Projecte de Llei orgànica de Protecció de dades personals (BOCCGG, de 24.11.2017), que es troba en fase de tramitació parlamentària, disposa, en el seu article 7, el següent:

> "Artículo 7. Consentimiento de los menores de edad.
>
> *1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de trece años.*
> *Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.*
> *(...).*

Atès que, com s'ha apuntat, la licitud del tractament de les dades d'aquests alumnes estaria fonamentada en el previ consentiment, l'Ajuntament haurà de demanar el consentiment als propis alumnes, en cas que siguin menors majors de 14 anys o, en el cas que es pugui tractar de menors que no tenen encara 14 anys, caldrà que l'Ajuntament disposi del consentiment dels seus pares o representants legals. Això sens perjudici de les condicions específiques que hagi establert el SMI per donar-se d'alta a l'aplicació.

En conclusió, el fet que l'Ajuntament disposi del consentiment de tots els participants en els Grups 1, 2 i 3, legitimaria no només la creació dels Grups, sinó, en lògica conseqüència, l'accés per part dels participants de cada Grup a les dades de la resta d'usuaris del grup (número de telèfon, foto o imatge de perfil,...), i a la informació que aquests comparteixin (missatges de text, missatges de veu, fotografies...), per a donar compliment a la finalitat específica dels diferents Grups.

VII

Dit això, l'Ajuntament pregunta si seria correcte (a més d'acotar al màxim la finalitat del grup), incloure una clàusula de polítiques de bon ús per part dels usuaris (ciutadans) del Grup, de compromís que no cediran a tercers ni telèfons del grup, ni la fotografia del perfil, ni tan sols les imatges que es puguin compartir en el grup (la consulta cita com a *exemple "que algun padre colgara en el grupo una foto en el que se identificara a los asistentes al evento, adultos y menores").*

D'entrada, com s'ha apuntat, la creació dels Grups de SMI (Casos 1, 2 i 3), tenen una finalitat clara i específica, que la pròpia consulta explica. Per aplicació del principi de finalitat (art. 4.2 LOPD), i tenint en compte que la normativa exigeix que les dades es tractin amb licitud, lleialtat i transparència (art. 5.1.a) RGPD), és clar que les dades han de ser recollides amb finalitats determinades, explícites i legítimes, i que no han de ser tractades ulteriorment de manera incompatible amb aquestes finalitats (art. 5.1.b) RGPD).

L'Ajuntament, com a responsable i administrador dels Grups, ha de preveure i explicar de forma adequada a les persones que en seran participants, quina és la finalitat de la comunicació del Grup, amb el màxim detall possible i de forma entenedora com, de fet, apunta la pròpia consulta.

Fem avinent que l'RGPD dona carta de naturalesa al principi de transparència (considerant 39 i considerant 58 RGPD). Segons disposa l'article 5.1.a) de l'RGPD, les dades han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat.

El principi de transparència, vinculat als principis de licitud i de lleialtat (art. 5.1.a) RGPD), engloba específicament el deure del responsable d'informar els afectats sobre una sèrie de qüestions, en els termes de l'article 13 RGPD, al que ens remetem, i que en alguns aspectes va més enllà del que disposa l'article 5 LOPD. Per tant, l'Ajuntament, com a responsable del tractament de dades de determinades persones físiques –als efectes que interessen, les persones que poden participar en els diferents Grups de SMI que creï l'Ajuntament-, els haurà d'informar sobre el dit tractament, entre d'altres, sobre la finalitat del mateix, i la base jurídica d'aquest tractament (art. 13.1.c) RGPD).

A partir de la data d'aplicació del RGPD, caldrà informar dels següents aspectes (article 13 RGPD): les dades de contacte del delegat de protecció de dades; la base jurídica del tractament; els interessos legítims perseguits en què es fonamenti el tractament; la intenció de transferir les dades a un país tercer o organització internacional i la base per a fer-ho; el termini durant el qual es conservaran les dades; l'existència del dret a demanar la portabilitat; el dret a retirar en qualsevol moment el consentiment que s'hagi prestat; si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte; el dret a presentar una

reclamació davant una autoritat de control; l'existència de decisions automatitzades, incloent la lògica aplicada i les seves conseqüències.

Les clàusules que no tenen en compte el grau de comprensió del ciutadà mig, sinó que, fins i tot, abusen de terminologia legal, no serien admissibles, segons afirma el GT29, en el document de Directrius sobre el consentiment (*"Guidelines on Consent under Regulation 2016/679",* de 28 de novembre de 2017): *"Al solicitar el consentimiento, los controladores deben garantizar que utilicen un lenguaje claro y sencillo en todos los casos. Esto significa que un mensaje debe ser fácilmente comprensible para la persona promedio y no solo para los abogados. Los controladores no pueden usar largas políticas de privacidad ilegibles o declaraciones llenas de jerga legal.*"

Als efectes que interessen en aquest dictamen, l'Ajuntament haurà de posar especial èmfasi en informar de forma entenedora als participants en els Grups, i prèviament a la posada en funcionament d'aquests Grups, d'una banda, sobre el fet que els participants en el Grup podran accedir a les dades de contacte de la resta de participants, i d'altra banda, sobre el fet que els participants podran accedir a la informació que continguin els missatges (escrits, de veu, arxius adjunts, fotografies...) que es comuniquin a través del Grup.

Pel que fa al compliment del deure d'informació en relació amb els menors d'edat que puguin formar part del Grup del Consell d'Infància (Cas 3), fem notar que, segons l'article 13.3 RLOPD: *"Quan el tractament es refereixi a dades de menors d'edat, la informació que s'hi adreci s'ha d'expressar en un llenguatge que els sigui fàcilment comprensible, amb expressa indicació del que disposa aquest article."* Segons el Considerant 58 de l'RGPD *"(...). Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender."*

Per tant, en relació amb els menors d'edat que puguin donar el consentiment per ells mateixos (menors majors de 14 anys, sens perjudici de les previsions que pugui contenir el Projecte de Llei orgànica de protecció de dades, a què ens hem referit, que es troba en seu parlamentària), la informació que se'ls faciliti haurà de ser especialment adaptada al seu nivell de comprensió.

VIII

La consulta pregunta sobre la responsabilitat que podria tenir l'Ajuntament respecte la cessió que puguin fer els participants dels Grups a tercers. Val a dir que la consulta es refereix, en aquest punt, als pares o ciutadans que participen als Grups.

En qualsevol cas, com a qüestió prèvia, convé distingir el tractament de dades per part de regidors o treballadors del propi Ajuntament que formin part dels Grups, del tractament que puguin fer els ciutadans (pares , alumnes, o membres d'associacions), que no tenen, en principi, i per la informació de què es disposa, cap vinculació laboral o orgànica amb el Consistori.

Com ha fet avinent aquesta Autoritat en Dictàmens anteriors, cal tenir en compte que si l'accés dels regidors a dades personals es produeix per raó de les funcions que com a tals tenen encomanades (com podria ser el cas, per la informació disponible, dels regidors a què es refereix la consulta), aquests han de regir-se pel deure de reserva imposat per la normativa de règim local (article 164.6 del Text de la Llei municipal i de

règim local de Catalunya, aprovat per Decret legislatiu 2/2003, de 28 d'abril (TRLMRLC), segons el qual *"els membres de la corporació han de respectar de la informació a què tenen accés per raó del càrrec si el fet de publicar-ho pot perjudicar els interessos de l'ens local o de tercers"*).

A banda d'aquesta previsió específica que afectaria els regidors, els treballadors municipals que, segons la consulta, podrien formar part dels Grups, estan vinculats pel deure de confidencialitat que els imposa la normativa com a treballadors públics (art. 52 de l'Estatut bàsic del treballador públic, aprovat per Reial Decret Legislatiu 5/2015, de 30 octubre (EBEP)), així com al deure general de secret que imposa l'article 10 LOPD, segons el qual: *"El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional pel que fa a les dades i al deure de guardar-les, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el seu responsable".*

A més, segons disposa el Codi Penal (articles 197 i 198), l'autoritat o funcionari públic que, fora dels casos permesos en la llei i prevalent-se del seu càrrec, difongui, reveli o cedeixi a tercers determinades dades, estaria realitzant una conducta que podria ser constitutiva del delicte de descobriment i revelació de secrets.

Això, juntament amb l'exigència derivada del principi de finalitat, comporta que els regidors i els treballadors de l'Ajuntament que, per raó del seu càrrec, puguin formar part dels Grups objecte de consulta, en cas de difondre a tercers, o tractar la informació (ja siguin dades de contacte d'altres membres del Grup, o altra informació personal), sense consentiment dels afectats i per a d'altres finalitats diferents de la pròpia del Grup, podrien contravenir la normativa de protecció de dades personals. Fins i tot pot derivar-se una responsabilitat disciplinària en determinats casos (art. 83 RGPD i art. 46.2 LOPD).

Per tant, l'Ajuntament sí podria tenir responsabilitat sobre un tractament inadequat que, per exemple, dugui a terme un treballador municipal que forma part del Grup i que hi intervé per raó del seu càrrec.

Pel que fa als pares de nens que acudeixen a la ludoteca, als membres d'associacions del poble o als menors d'edat de les escoles, tot i que la creació dels Grups 1, 2 i 3, sigui a iniciativa de l'Ajuntament, difícilment aquest tindria responsabilitat directa (als efectes de l'article 46 LOPD), sobre l'ús posterior que persones alienes a l'Ajuntament facin de dades personals (comentaris, números de contacte, fotos...), a què hauran accedit legítimament, en els termes apuntats.

Dit això, cal tenir en compte que, en principi, qualsevol persona que accedeix a dades personals d'altri per a una finalitat legítima, hauria de tractar les dades personals a què hagi pogut accedir conforme als principis i garanties de la normativa de protecció de dades, citats.

Així, en principi, els ciutadans que participen en els Grups haurien de tractar les dades personals a què tinguin accés en el marc de la finalitat pròpia del Grup. Els membres del Grup haurien de disposar del consentiment o una altra habilitació legal per comunicar a persones alienes al mateix, la informació personal que s'hi tracta. El deure general de secret (art. 5.1.f) RGPD i art. 10 LOPD) també resultaria d'aplicació en aquest cas. A tall d'exemple, per comunicar el número de telèfon d'un altre membre del Grup a una tercera persona aliena a aquest, caldria el seu consentiment.

En el cas concret de la imatge de les persones, que és una dada personal (art. 5.1.f) RLOPD), com ha fet avinent aquesta Autoritat en ocasions anteriors (Dictàmens CNS 9/2016, o CNS 64/2015, entre d'altres), la captació i difusió de la imatge gràfica de persones identificades o identificables afecta al dret a la pròpia imatge (art. 18.1 CE) i, per tant, cal tenir en compte la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge (LO 1/1982). Les previsions de l'LO 1/1982 (arts. 7.5 i 8.2), podrien habilitar la captació i difusió d'imatges de persones identificables (per exemple, a través de fotografies) en un acte públic i en què la imatge d'aquestes persones aparegui com a merament accessòria. De ser així, no seria estrictament necessari, des del punt de vista de la normativa estudiada, disposar del consentiment previ dels afectats, per tal que els membres del Grups poguessin cedir a tercers imatges d'aquest tipus. En canvi, en altres tipus d'imatges en què no es donin aquests elements caldria disposar del consentiment dels afectats.

En qualsevol cas, i sens perjudici d'aquesta puntualització, no resultaria contrari a la normativa de protecció de dades i, fins i tot, podria ser recomanable, que l'Ajuntament estableixi, com política de bon ús, que els membres dels Grups no comparteixin imatges amb tercers aliens al Grup, llevat que disposin dels consentiments que puguin ser necessaris, atesa la normativa citada.

Deixant de banda les fotografies, i en referència a d'altres tipus d'informacions que es puguin compartir en els Grups, resulta convenient que l'Ajuntament adverteixi als participants dels Grups que compartir amb tercers informació especialment protegida (com podrien ser dades de salut, possibilitat que apunta la consulta) podria contravenir les previsions de la normativa de protecció de dades personals. En aquest punt, a efectes il·lustratius, i per la seva rellevància, ens remetem a la Sentència B. Lindqvist, del Tribunal de Justícia de la UE, de 6 de novembre de 2003. Això, sens perjudici que, per la informació de què es disposa, no sembla que la finalitat dels Grups 1, 2 i 3 faci probable el tractament d'informació especialment protegida.

Per tot l'exposat, atesa la problemàtica que planteja la consulta (possible difusió de fotografies, comentaris, etc, per part dels participants), cal valorar positivament que l'Ajuntament elabori una "clàusula de polítiques de bon ús" (un codi de bones pràctiques, en definitiva), per tal que tots els participants en els Grups (independentment de la seva vinculació o no amb l'Ajuntament) tractin les dades personals objecte de consulta de forma ajustada a les previsions de la normativa citada.

Finalment, pel que fa a la possibilitat d'expulsar algun membre del Grup, a què es refereix la consulta, des de la perspectiva de la protecció de dades no correspon a aquesta Autoritat determinar en quins casos l'Ajuntament ha de prendre la decisió d'expulsar un membre d'algun dels Grups 1, 2 i 3.

Ara bé, el mer fet d'haver expulsat un membre del Grup de SMI, no desvirtua l'obligació de l'Ajuntament de donar compliment dels principis i obligacions, en matèria de protecció de dades, que li puguin correspondre com a responsable, ni tampoc les conseqüències que un tractament inadequat de les dades personals pugui comportar.

IX

El Cas 4, fa referència a un Grup de Whatsapp que, segons la informació de què es disposa, no crearia l'Ajuntament, sinó "els joves del poble", tot i que, segons la consulta, s'hauria afegit a aquest Grup un treballador municipal, utilitzant un número

de telèfon del propi Ajuntament. L'Ajuntament pregunta si, en no ser administrador del Grup, l'Ajuntament tindria alguna responsabilitat com a Administració, i si hauria de realitzar alguna gestió en referència a l'LOPD.

Atesa la informació disponible, cal fer avinent que es desconeix la finalitat del Grup en qüestió, és a dir, si aquest podria tenir alguna relació, directa o indirecta, amb alguna activitat o servei que presta o organitza l'Ajuntament. Es desconeix si en el marc d'aquest Grup es podria tractar determinada informació personal de la que en sigui responsable l'Ajuntament. També es desconeix si el treballador municipal que, segons la consulta, s'hauria afegit al Grup, en formaria part en la seva condició de treballador de l'Ajuntament i per raó de la seva feina, o bé a títol particular.

En relació amb aquesta qüestió, el RGPD disposa que aquest Reglament no s'aplica al tractament de dades personals efectuat per una persona física en l'exercici d'activitats exclusivament personals o domèstiques (Considerant 18 i art. 2.2.c) RGPD).Es manté així l'exclusió que ja contenia l'LOPD respecte els tractaments mantinguts per persones físiques en exercici d'activitats exclusivament personals o domèstiques (art. 2.2.a) LOPD), entenent com a tals les que s'inscriuen en el marc de la vida privada o familiar dels particulars (art. 4.a) RLOPD) o, com va precisar l'Audiència Nacional en Sentència de 15 de juny de 2006: *"(...) Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos."*

Per tant, atesa la informació de què es disposa, aquesta Autoritat no pot determinar si el Grup referit (Cas 4) té una finalitat exclusivament personal o domèstica i, en conseqüència, si el tractament de dades que s'hi pugui fer es troba o no subjecte a la normativa de protecció de dades personals.

Per altra banda, per la informació aportada sembla clar que no es tractaria d'un tractament responsabilitat de l'Ajuntament, amb independència que un determinat treballador de la corporació s'hi hagi afegit a títol particular.

En qualsevol cas, el treballador, atesa la seva vinculació laboral amb l'Ajuntament, té l'obligació de tractar la informació personal de què pugui ser coneixedor per raó del seu càrrec, amb ple respecte pels principis i garanties de la normativa de protecció de dades, atesa la normativa citada.

D'acord amb les consideracions fetes en aquest dictamen, es fan les següents,

Conclusions

A l'hora d'establir la utilització d'un determinat canal de comunicació en els serveis municipals, l'Ajuntament ha de tenir en compte les garanties que ofereix el canal per al tractament de la informació de les persones afectades i l'existència o no d'altres canals alternatius.

Casos 1, 2 i 3: L'Ajuntament ha de donar compliment als principis i garanties de la normativa de protecció de dades, entre d'altres, ha de disposar del consentiment de tots els participants dels Grups, llevat que compti amb una altra base jurídica i donar-los informació sobre el tractament de les dades (art. 13 RGPD) i les conseqüències que es poden derivar de la utilització d'aquest canal.

Tot i que la creació dels Grups sigui a iniciativa de l'Ajuntament, difícilment aquest tindria responsabilitat directa (als efectes de l'article 46 LOPD), sobre l'ús posterior que persones alienes a l'Ajuntament facin de dades personals. Sens perjudici d'això, es valora positivament l'elaboració d'una "clàusula de polítiques de bon ús", per tal que tots els participants en els Grups tractin les dades personals de forma ajustada a les previsions de la normativa.

Cas 4: Atesa la informació disponible, no es pot determinar si el Grup té una finalitat exclusivament personal o domèstica i, en conseqüència, si es troba o no subjecte a la normativa de protecció de dades personals. En qualsevol cas, per la informació facilitada, no seria responsabilitat de l'Ajuntament.

Barcelona, 26 d'abril de 2018