DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 32| Febrer 2023

Aplicacions de missatgeria instantània en el sector públic

Í N D E X

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades y Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ

A manera d'introducció, cal fer notar que els mitjans o serveis de comunicació que poden utilitzar les administracions públiques ja siga per a relacionar-se amb els ciutadans o amb altres administracions públiques, o com a canal de comunicació intern dins de la seua pròpia estructura; poden ser de naturalesa molt variada: mitjans de comunicació tradicionals (premsa, ràdio o televisió), webs pròpies, intranets corporatives, correu ordinari, telèfon, comunicació presencial, etc.

No obstant això, en els últims anys les aplicacions de missatgeria instantània com WhatsApp o Telegram, s'han convertit en instruments essencials per a les administracions públiques. Aquest tipus d'aplicacions, són utilitzades per part de les administracions, de dues formes possibles:

- Ús com a canal bidireccional: moltes administracions han implementat un telèfon amb Whatsapp o Telegram com a mètode de contacte; perquè els ciutadans puguen compartir els seus suggeriments o dubtes. Aquest tipus de canal, ofereix una imatge molt positiva de l'Administració, a causa de la immediatesa del servei i a la sensació de proximitat generada en els ciutadans.
- Ús com a canal unidireccional: algunes aplicacions com Telegram o Whatsapp (a través de la modalitat “llista de difusió), ofereixen la possibilitat d'enviar missatges a través d'un "canal", sense que cap integrant del canal tinga la possibilitat de respondre al remitent original. Aquesta característica pot ser utilitzada com un canal de comunicació oficial de l'Administració amb els ciutadans, de manera que tots els usuaris adscrits; reben una notificació en el seu telèfon sobre les últimes novetats de l'Administració a la qual pertanyen.

No obstant això, la utilització d'aquesta mena d'aplicacions pot implicar que l'administració incórrega en alguna infracció de la normativa vigent en matèria de protecció de dades. Per això, és necessari que l'administració local, tinga en compte una sèrie de circumstàncies.

En el present butlletí s'analitzaran les possibles implicacions derivades de l'ús d'aquesta mena d'aplicacions.

Una Administració pública pot comunicar-se amb la ciutadania mitjançant WhatsApp o un altre servei de missatgeria instantània? Respostes de les autoritats

A continuació, s'exposen en termes generals, les opinions de les diverses autoritats de control del territori espanyol:

- **Agència Espanyola de Protecció de Dades (d'ara en avant, AEPD):**

En la Guia "Protecció de dades i administració local", l'AEPD no descarta el seu ús per part de les Administracions públiques, però exigeix que siga tingut en compte el principi de finalitat del **Reglament General de Protecció de Dades (d'ara en avant, RGPD)**; en connexió amb el principi de licitud, lleialtat i transparència (el qual implica l'existència d'una base de legitimació per a tractar les dades personals, i el deure d'informar sobre el citat tractament als afectats).

Sobre aquest tema, posa el següent exemple:

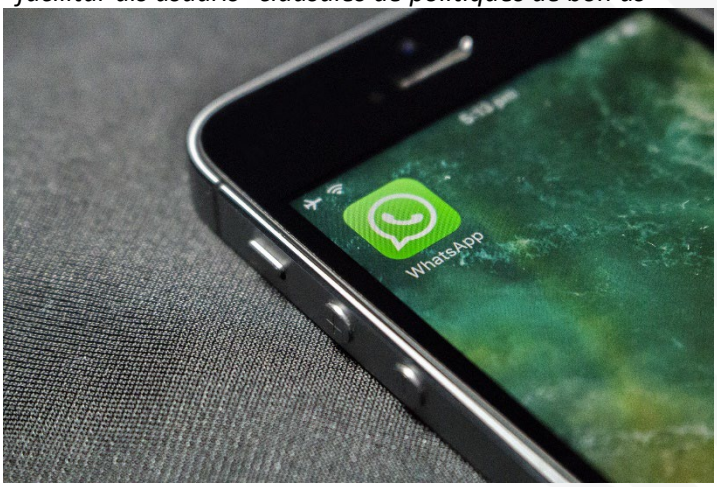
"Si l'ens local haguera recaptat la dada del mòbil per a una finalitat determinada (per exemple, en la presentació d'una denúncia), l'ús d'aquesta dada per a enviar aquestes comunicacions seria incompatible, per la qual cosa per a realitzar el citat enviament seria necessari ***el consentiment previ dels ciutadans, a més d'informar-los del tractament*** *que es realitzarà respecte a aqueixa dada de caràcter personal"*

- **Autoritat Catalana de Protecció de dades (d'ara en avant, APDCAT):**

L'**APDCAT**, en si dictamen CNS 13/2018 admet l'ús d'aquesta mena d'aplicacions, sempre que les mateixes s'ajusten a les *"exigències de la normativa de protecció de dades".*

En aquest sentit, l'**APDCAT** posa el focus també en els principis de licitud, lleialtat i transparència indicant que:

"Si l'Administració utilitza grups de WhatsApp o un altre servei de missatgeria instantània per a comunicar-se amb els ciutadans, haurà de disposar del consentiment de tots els membres del grup, llevat que compte amb una altra base jurídica, i els informarà sobre el tractament de les dades i les conseqüències que es poden derivar de la utilització d'aquest canal. A aquest efecte, l'Administració pot facilitar als usuaris "clàusules de polítiques de bon ús"



Així mateix, respecte a l'ús del **consentiment com a base de legitimació** indica que, perquè el mateix siga considerat com a lliure, tal com exigeix la normativa, *"és necessari que les persones participants tinguen* ***altres canals alternatius de comunicació amb l'Administració*** *per a les finalitats previstes; és a dir, el servei de missatgeria instantània no se'ls imposarà com a única via de comunicació"*.

Resolucions rellevants sobre la creació de grups i llistes de difusió per Whatsapp per les Administracions Públiques: Cas Ajuntament de Tiana

Tant l'AEPD, com les autoritats autonòmiques de protecció de dades, s'han pronunciat sobre el fet que una autoritat (en aquest cas, Ajuntaments), poguera crear grups de difusió d'informació a través d'aplicacions de missatgeria instantània com WhatsApp.

Tal com hem explicat al principi del present butlletí, un grup de WhatsApp constituiria una comunicació bidireccional; mentre que una llista de difusió seria una comunicació unidireccional.

Sobre aquest tema podem destacar **dues resolucions**:

1. **RESOLUCIÓ: R/03041/2017: Ajuntament de Boecillo (Valladolid)**

En aquest cas l'Ajuntament, va ser amonestat per crear un grup de WhatsApp en el qual un regidor del consistori va incloure a 255 persones per a informar-los de possibles temes d'interés del municipi sense "*consentiment ni autorització per a aquest tractament"*.

La resolució se centra en que el tractament de dades era **contrari al principi de qualitat de l'anterior normativa** (el qual prohibeix utilitzar dades per a una finalitat incompatible o diferent d'aquella per a la qual els mateixos van ser recaptats; equivalent a l'actual principi de finalitat), i el **deure de secret de l'anterior normativa** ja que "*que els números de telèfon dels integrants del grup de WhatsApp eren visibles per a tots els altres membres del grup*".

2. **RESOLUCIÓ: PS 28/2021, referent a l'Ajuntament de Tiana (Barcelona)**

En aquest cas, l'Ajuntament de Tiana, malgrat comptar amb el consentiment explícit de cadascun dels components del grup de WhatsApp i d'informar-los com serien tractats les seues dades personals, és sancionat per l'APDCAT al no tindre en compte **l'art. 25 del RGPD; la "*Protecció de dades des del disseny i per defecte*"**.

Aquesta resolució és important per distingir entre "*grup*" i "*llista de difusió*", sent totes dues funcions de WhatsApp similars entre si sense arribar a ser el mateix.

El principal error que va cometre l'entitat municipal va ser "*no implantar mesures tècniques i organitzatives adequades per a aplicar de manera efectiva el principi de confidencialitat*". En concret, no es garantia que les persones que es van unir al grup de WhatsApp creat per l'Ajuntament, "*no pogueren accedir al número de mòbil, foto de perfil i nom d'usuari de la resta de membres*".

Tal com indica l'APDCAT, aquesta infracció es podria haver evitat si l'ajuntament "*crea una llista de difusió els missatges enviats apareixen en cada contacte de la llista de difusió com un missatge individual*". Gràcies a això, "*les persones incloses en la llista de difusió desconeixen qui són els altres integrants de la llista i, per tant, no poden accedir a les dades de la resta*", no sent idònia la funcionalitat dels grups per a aquestes finalitats.

Com es pot observar, la sanció en aquest cas deriva del fet que un grup de WhatsApp exposa necessàriament les dades dels integrants, vulnerant la normativa. És a dir, el que se li retrau a l'ajuntament és que no adoptara les mesures necessàries per a impedir que els usuaris del grup tingueren accés a les dades personals de la resta de participants; a pesar que no tenia per què prescindir de l'aplicació: hauria bastat amb optar per una altra funcionalitat diferent de l'aplicació, les "*llistes de*

difusió".

Principi de responsabilitat proactiva i transferències internacionals de dades

Hem de recordar que de conformitat amb el **principi de responsabilitat proactiva de l'article 5 del RGPD**; els responsables de tractament (Exemple: Ajuntaments); han d'aplicar mesures tècniques i organitzatives apropiades a fi de **garantir i poder demostrar que el tractament és conforme amb el Reglament.**

En aquest sentit, **l'article 28 del RGPD**, estableix l'obligació per als responsables de tractament, de triar únicament a aquells encarregats que **oferisquen garanties suficients per a aplicar mesures tècniques i organitzatives apropiades,** de tal manera que el tractament que realitzen per compte del responsable siga conforme amb els requisits establits en la citada normativa.

D'altra banda, a nivell nacional ha de destacar-se la disposició addicional primera **Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD)**; la qual prescriu la implantació de les mesures de seguretat de **l'Esquema Nacional de Seguretat** a les entitats del sector públic i a les del sector privat que col·laboren amb aquestes en la prestació de serveis públics que involucren el tractament de dades personals.

Transferències internacionals de dades

Ha de tindre's en compte, que algunes de les companyies que hem citat, tenen la seua matriu fora de l'Espai Econòmic Europeu, en territoris que actualment no ofereixen un nivell equivalent de protecció a l'atorgat pel RGPD (com pot ser Unió dels Emirats Àrabs, en cas de Telegram, o els EUA en el cas de WhatsApp).

Tal com es regula en el RGPD, aquestes transferències només poden ser dutes a terme si existeixen una **sèrie de garanties**; com la signatura de les clàusules contractuals tipus, o l'existència d'unes normes corporatives vinculants. Al costat de l'existència d'aquestes garanties, els responsables han **d'avaluar si la legislació d'aqueixos tercers països assegura l'eficàcia** de la garantia triada; i en cas de no estar assegurada, imposar **mesures addicionals**.

Per tant, tota **entitat pública que vaja a recórrer un proveïdor de missatgeria instantània que transmeta dades fora de l'Espai Econòmic Europeu, ha de:**

1. Cerciorar-se a través dels textos legals del proveïdor de l'existència de **garanties en matèria de transferències internacionals.**
2. **Analitzar**, si malgrat les garanties, la legislació del país no permet la seua **plena eficàcia**. Exemple: llei del país de destinació que permet a les seues autoritats d'intel·ligència exigir accés a les dades de les empreses allí radicades.
3. **Si no** permet garantir la seua eficàcia, existeixen **dues opcions**:

- Suspendre la transferència (i, per tant, no contractar el proveïdor).
- Imposar mesures addicionals.

En aquest sentit, en alguns territoris s'ha considerat que no és segur utilitzar algunes d'aquestes aplicacions precisament pel fet de realitzar transferències internacionals a territoris que no permetien assegurar un nivell adequat de protecció.

Aquest ha sigut el cas d'Alemanya, on el comissionat de protecció de dades alemany ha prohibit l'ús de WhatsApp, per part de qualsevol autoritat federal, per a evitar possibles filtracions indesitjades d'informació confidencial.

MATERIAL COMPLEMENTARI

- Guia de Protecció de Dades i Administració Local. Consulta aquest enllaç.
- Recomanacions 01/2020 sobre mesures que complementen els instruments de transferència per a garantir el compliment del nivell de protecció de les dades personals de la UE (CEPD). Consulta aquest enllaç.
- Guia de privacitat i seguretat en Internet (AEPD, INCIBE, OSI). Consulta aquest enllaç.

NOTÍCIES

- **L'AEPD es posiciona en favor de la legitimitat de l'ús de grups de WhatApp sense consentiment en l'àmbit laboral**

En una resolució del 9 de gener de 2023, l'AEPD, ha considerat que aquest tractament queda emparat en el contracte laboral signat entre l'empresari que crea el grup de Whatsapp i els treballadors; entenent per tant que no és necessari comptar amb el consentiment previ dels interessats.

La resolució porta causa en una reclmación d'un empleat d'Ariathor Logistics S.L. L'empresa va incloure al treballador en dos grups de WhatsApp, en els quals es publicaven "*dades relatives a les rutes de repartiment, les persones que la realitzen, les hores, la ubicació de les furgonetes en acabar la jornada laboral i diversa informació laboral*".

L'AEPD assenyala que el tractament de dades és mínim perquè no comporta un ús d'informació excessiu en tractar-se d'una fi determinada (“*utilitzar aquesta via de comunicació en assumptes relacionats amb el contracte de treball, condicions laborals, organització i desenvolupament de tasques de treball i repartiment i mantenint la confidencialitat sobre ells*”); i que a més, l'ús d'aquesta aplicació és essencial per al treball.

Consulta la resolució en aquest enllaç.