DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 32| Febrero 2023

Aplicaciones de mensajería instantánea en el sector público

Í N D I C E

APLICACIONES DE MENSAJERÍA INSTANTÁNEA EN EL SECTOR PÚBLICO

	Página
Introducción	**2**
¿Una Administración pública puede comunicarse con la ciudadanía mediante WhatsApp u otro servicio de mensajería instantánea? Respuestas de las autoridades	**3**
Resoluciones relevantes sobre la creación de grupos y listas de difusión por WhatsApp por las Administraciones Públicas: Caso Ayuntamiento de Tiana	**4**
Principio de responsabilidad proactiva y transferencias internacionales de datos	**5**
Noticias y material complementario	**7**

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

A modo de introducción, hay que hacer notar que los medios o servicios de comunicación que pueden utilizar las administraciones públicas ya sea para relacionarse con los ciudadanos o con otras administraciones públicas, o como canal de comunicación interno dentro de su propia estructura; pueden ser de naturaleza muy variada: medios de comunicación tradicionales (prensa, radio o televisión), webs propias, intranets corporativas, correo ordinario, teléfono, comunicación presencial, etc.

Sin embargo, en los últimos años las aplicaciones de mensajería instantánea como WhatsApp o Telegram, se han convertido en instrumentos esenciales para las administraciones públicas. Este tipo de aplicaciones, son utilizadas por parte de las administraciones, de dos formas posibles:

- Uso como canal bidireccional: muchas administraciones han implementado un teléfono con Whatsapp o Telegram como método de contacto; para que los ciudadanos puedan compartir sus sugerencias o dudas. Este tipo de canal, ofrece una imagen muy positiva de la Administración, debido a la inmediatez del servicio y a la sensación de cercanía generada en los ciudadanos.
- Uso como canal unidireccional: algunas aplicaciones como Telegram o Whatsapp (a través de la modalidad *"lista de difusión*), ofrecen la posibilidad de enviar mensajes a través de un *"canal",* sin que ningún integrante del canal tenga la posibilidad de responder al remitente original. Esta característica puede ser utilizada como un canal de comunicación oficial de la Administración con los ciudadanos, de forma que todos los usuarios adscritos; reciban una notificación en su teléfono sobre las últimas novedades de la Administración a la que pertenecen.

No obstante, la utilización de este tipo de aplicaciones puede acarrear que la administración incurra en alguna infracción de la normativa vigente en materia de protección de datos. Por ello, es necesario que la administración local, tenga en cuenta una serie de circunstancias.

En el presente boletín se analizarán las posibles implicaciones derivadas del uso de este tipo de aplicaciones.

¿Una Administración pública puede comunicarse con la ciudadanía mediante WhatsApp u otro servicio de mensajería instantánea? Respuestas de las autoridades

A continuación, se exponen en términos generales, las opiniones de las diversas autoridades de control del territorio español:

- **Agencia Española de Protección de Datos (en adelante, AEPD):**

En la Guía "*Protección de datos y administración local",* la AEPD no descarta su uso por parte de las Administraciones públicas, pero exige que sea tenido en cuenta el principio de finalidad del **Reglamento General de Protección de Datos (en adelante, RGPD)**; en conexión con el principio de licitud, lealtad y transparencia (el cual implica la existencia de una base de legitimación para tratar los datos personales, y el deber de informar sobre el citado tratamiento a los afectados).

Al respecto, pone el siguiente ejemplo:

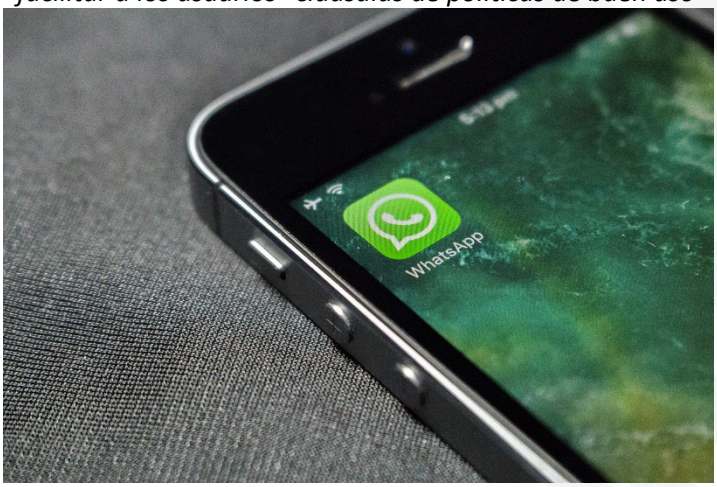
"Si el ente local hubiese recabado el dato del móvil para una finalidad determinada (por ejemplo, en la presentación de una denuncia), el uso de este dato para enviar dichas comunicaciones sería incompatible, por lo que para realizar el citado envío sería necesario ***el consentimiento previo de los ciudadanos****,* ***además de informarles del tratamiento*** *que se va a realizar respecto a ese dato de carácter personal"*

- **Autoridad Catalana de Protección de datos (en adelante, APDCAT):**

La **APDCAT**, en si dictamen CNS 13/2018 admite el uso de este tipo de aplicaciones, siempre y cuando las mismas se ajusten a las *"exigencias de la normativa de protección de datos".*

En este sentido, la **APDCAT** pone el foco también en los principios de licitud, lealtad y transparencia indicando que:

"Si la Administración utiliza grupos de WhatsApp u otro servicio de mensajería instantánea para comunicarse con los ciudadanos, deberá disponer del consentimiento de todos los miembros del grupo, a menos que cuente con otra base jurídica, y les informará sobre el tratamiento de los datos y las consecuencias que se pueden derivar de la utilización de este canal. Con este fin, la Administración puede facilitar a los usuarios "cláusulas de políticas de buen uso"



Asimismo, respecto al uso del **consentimiento como base de legitimación** indica que, para que el mismo sea considerado como **libre**, tal y como exige la normativa, "*es necesario que las personas participantes tengan* ***otros canales alternativos de comunicación con la Administración*** *para las finalidades previstas; es decir, el servicio de mensajería instantánea no se les impondrá como única vía de comunicación".*

Resoluciones relevantes sobre la creación de grupos y listas de difusión por Whatsapp por las Administraciones Públicas: Caso Ayuntamiento de Tiana

Tanto la AEPD, como las autoridades autonómicas de protección de datos, se han pronunciado sobre el hecho de que una autoridad (en este caso, Ayuntamientos), pudiera crear grupos de difusión de información a través de aplicaciones de mensajería instantánea como WhatsApp.

Tal y como hemos explicado al principio del presente boletín, un grupo de WhatsApp constituiría una comunicación bidireccional; mientras que una lista de difusión sería una comunicación unidireccional.

Al respecto podemos destacar **dos resoluciones:**

1. **RESOLUCIÓN: R/03041/2017: Ayuntamiento de Boecillo (Valladolid)**

En este caso el Ayuntamiento, fue amonestado por crear un grupo de WhatsApp en el que un concejal del consistorio incluyó a 255 personas para informarles de posibles temas de interés del municipio sin *"consentimiento ni autorización para dicho tratamiento"*.

La resolución se centra en que el tratamiento de datos era **contrario al principio de calidad de la anterior normativa** (el cual prohíbe utilizar datos para una finalidad incompatible o distinta de aquella para la que los mismos fueron recabados; equivalente al actual principio de finalidad), y el **deber de secreto de la anterior normativ**a ya que *"que los números de teléfono de los integrantes del grupo de WhatsApp eran visibles para todos los demás miembros del grupo"*.

2. **RESOLUCIÓN: PS 28/2021, referente al Ayuntamiento de Tiana (Barcelona)**

En este caso, el Ayuntamiento de Tiana, a pesar de contar con el consentimiento explícito de cada uno de los componentes del grupo de WhatsApp y de informarles cómo serían tratados sus datos personales, es sancionado por la APDCAT al no tener en cuenta el **art. 25 del RGPD; la *"Protección de datos desde el diseño y por defecto"*.**

Esta resolución es importante por distinguir entre *"grupo"* y *"lista de difusión*", siendo ambas funciones de WhatsApp similares entre sí sin llegar a ser lo mismo.

El principal error que cometió la entidad municipal fue *"no implantar medidas técnicas y organizativas adecuadas para aplicar de forma efectiva el principio de confidencialidad"*. En concreto, no se garantizaba que las personas que se unieron al grupo de WhatsApp creado por el Ayuntamiento*, "no pudieran acceder al número de móvil, foto de perfil y nombre de usuario del resto de miembros*"

Tal y como indica la APDCAT, esta infracción se podría haber evitado si el ayuntamiento "*crea una lista de difusión los mensajes enviados aparecen en cada contacto de la lista de difusión como un mensaje individual"*. Gracias a ello, *"las personas incluidas en la lista de difusión desconocen quiénes son los otros integrantes de la lista y, por tanto, no pueden acceder a los datos del resto",* no siendo idónea la funcionalidad de los grupos para estas finalidades.

Como se puede observar, la sanción en este caso deriva del hecho que un grupo de WhatsApp expone necesariamente los datos de los integrantes, vulnerando la normativa. Es decir, lo que se le reprocha al ayuntamiento es que no adoptase las medidas necesarias para impedir que los usuarios del grupo tuvieran acceso a los datos personales del resto de participantes; a pesar de que no tenía por qué

prescindir de la aplicación: hubiera bastado con optar por otra funcionalidad distinta de la aplicación, las "*listas de difusión".*

Principio de responsabilidad proactiva y transferencias internacionales de datos

Debemos recordar que de conformidad con el **principio de responsabilidad proactiva del artículo 5 del RGPD**; los responsables de tratamiento (Ejemplo: Ayuntamientos); deben aplicar medidas técnicas y organizativas apropiadas a fin de **garantizar y poder demostrar que el tratamiento es conforme con el Reglamento**

En este sentido, **el artículo 28 del RGPD**, establece la obligación para los responsables de tratamiento, de elegir únicamente a aquellos encargados que **ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas**, de tal manera que el tratamiento que realicen por cuenta del responsable sea conforme con los requisitos establecidos en la citada normativa.

Por otro lado, a nivel nacional ha de destacarse la disposición adicional primera **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**; la cual prescribe la implantación de las medidas de seguridad del **Esquema Nacional de Seguridad** a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales.

Transferencias internacionales de datos

Ha de tenerse en cuenta, que algunas de las compañías que hemos citado, tienen su matriz fuera del Espacio Económico Europeo, en territorios que actualmente no ofrecen un nivel equivalente de protección al otorgado por el RGPD (como puede ser Emiratos Árabes Unidos, en caso de Telegram, o EE. UU. en el caso de WhatsApp).

Tal y como se regula en el RGPD, estas transferencias sólo pueden ser llevadas a cabo si existen una **serie de garantías**; como la firma de las cláusulas contractuales tipos, o la existencia de unas normas corporativas vinculantes. Junto a la existencia de estas garantías, los responsables han de **evaluar si la legislación de esos terceros países asegura la eficacia** de la garantía escogida; y en caso de no estar asegurada, imponer **medidas adicionales**.

Por lo tanto, toda **entidad pública que vaya a recurrir un proveedor de mensajería instantánea que transmita datos fuera del Espacio Económico Europeo, ha de:**

1. Cerciorarse a través de los textos legales del proveedor de la existencia de **garantías en materia de transferencias internacionales.**
2. **Analizar,** si a pesar de las garantías, la legislación del país no permite su **plena eficacia**. Ejemplo: ley del país de destino que permite a sus autoridades de inteligencia exigir acceso a los datos de las empresas allí radicadas.

3. **Si no** permite garantizar su eficacia, existen **dos opciones**:
    - Suspender la transferencia (y, por lo tanto, no contratar el proveedor).
    - Imponer medidas adicionales.

En este sentido, en algunos territorios se ha considerado que no es seguro utilizar algunas de estas aplicaciones precisamente por el hecho de realizar transferencias internacionales a territorios que no permitían asegurar un nivel adecuado de protección.

Este ha sido el caso de Alemania, donde el comisionado de protección de datos alemán ha prohibido el uso de WhatsApp, por parte de cualquier autoridad federal, para evitar posibles filtraciones indeseadas de información confidencial.

MATERIAL COMPLEMENTARIO

- Guía de Protección de Datos y Administración Local. Consulta este enlace.
- Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE (CEPD). Consulta este enlace.
- Guía de privacidad y seguridad en Internet (AEPD, INCIBE, OSI). Consulta este enlace.

NOTICIAS

- **La AEPD se posiciona en favor de la legitimidad del uso de grupos de WhatApp sin consentimiento en el ámbito laboral**

  En una resolución del 9 de enero de 2023, la AEPD, ha considerado que dicho tratamiento queda amparado en el contrato laboral firmado entre el empresario que crea el grupo de Whatsapp y los trabajadores; entendiendo por lo tanto que no es necesario contar con el consentimiento previo de los interesados.

  La resolución trae causa en una reclmación de un empleado de Ariathor Logistics S.L. La empresa incluyó al trabajador en dos grupos de WhatsApp, en los que se publicaban *"datos relativos a las rutas de reparto, las personas que la realizan, las horas, la ubicación de las furgonetas al terminar la jornada laboral y diversa información laboral*".

  La AEPD señala que el tratamiento de datos es mínimo porque no conlleva un uso de información excesivo al tratarse de un fin determinado *("utilizar esta vía de comunicación en asuntos relacionados con el contrato de trabajo, condiciones laborales, organización y desarrollo de tareas de trabajo y reparto y manteniendo la confidencialidad sobre ellos"*); y que además, el uso de esta aplicación es esencial para el trabajo.

  Consulta la resolución en este enlace.