DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 13 | Julio 2021

DIRECTRICES PARA LA CORRECTA UTILIZACIÓN DE REDES SOCIALES CORPORATIVAS

Í N D I C E

DIRECTRICES PARA LA CORRECTA UTILIZACIÓN DE REDES SOCIALES CORPORATIVAS

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 suscribirte a nuestra publicación accede al siguiente

enlace

"A DIFERENCIA DE LOS SITIOS WEB GESTIONADOS DIRECTA O INDIRECTAMENTE POR LAS PROPIAS ADMINISTRACIONES PÚBLICAS, Y SOBRE LOS QUE ES POSIBLE UN CONTROL TOTAL DEL CONTENIDO Y DEL TIPO DE SERVICIO PRESTADO, LA RED SOCIAL ES UN ENTORNO QUE NO ESTÁ PENSADO INICIALMENTE PARA EL USO ADMINISTRATIVO. EN CUALQUIER CASO, SUPONE UN TRATAMIENTO DE DATOS PERSONALES QUE DEBE CUMPLIR CON LA NORMATIVA DE PROTECCIÓN DE DATOS".

INTRODUCCIÓN

Las redes sociales son uno de los canales de información más usados en Internet. Los usuarios encuentran en ellas un canal sencillo, accesible e inmediato por el que pueden compartir contenidos, socializar o incluso ofrecer un escaparate para dar a conocer sus productos o servicios.

La relación de las Administraciones Públicas con las redes sociales puede tomar muchas formas. La más conocida sería la presencia de perfiles 'oficiales' de los organismos en redes sociales abiertas, aunque no pueden obviarse otros usos como las redes sociales cerradas utilizadas como vehículo de comunicación interna, las redes o grupos no oficiales de empleados, o los empleados que publican en redes sociales a título individual.

A diferencia de los sitios web gestionados directa o indirectamente por las propias Administraciones Públicas, y sobre los que es posible un control total del contenido y del tipo de servicio prestado, la red social es un entorno que no está pensado inicialmente para el uso administrativo.

En cualquier caso, su utilización supone un tratamiento de datos personales que debe cumplir con la normativa de protección de datos.

A continuación, se ofrecen una serie de directrices para el correcto uso de las redes sociales corporativas, tanto de forma interna como para la oferta de servicios a los ciudadanos. Asimismo, se hará un repaso a algunos de los principales riesgos para los derechos y libertades de los interesados, asociados al uso de las redes sociales.

"LOS LÍMITES DE USOS DE REDES SOCIALES HAN DE QUEDAR CLARAMENTE DEFINIDOS EN LA POLÍTICA INTERNA DE LA ENTIDAD. SI EN LA POLÍTICA SE ADMITEN ESTE TIPO DE CANALES DE COMUNICACIÓN, SE ESTÁ ADMITIENDO UN TRATAMIENTO DEL QUE SERÁ RESPONSABLE LA ENTIDAD Y, POR LO TANTO, HABRÁ DE CUMPLIR CON LOS ESTABLECIDO EN EL RGPD Y EN EL ENS".

USO DE REDES SOCIALES DE FORMA INTERNA

En el uso interno de las redes sociales, podemos encontrarnos con redes cerradas, pensadas para los empleados como una evolución de las intranets corporativas a las que se han añadido rasgos sociales. Estas redes se apoyan en paquetes de software específicos y el acceso está restringido o incluso prohibido a terceros.

Otro posible uso interno de las redes sociales es el que resulta de las comunicaciones informales de los empleados, que forman grupos para hablar o intercambiar mensajes y noticias. Este tipo de redes a veces surge de forma espontánea y otras veces puede ser promovido por las propias organizaciones. Nos podemos encontrar con empleados de una misma entidad (y a veces también junto con exempleados y externos) que tratan asuntos profesionales entre ellos a través de una red insegura sin ser, muchas veces, conscientes de ello. Un empleado, de manera inconsciente y sin valorar los riesgos que representa, puede llegar incluso a confundir la red social de compañeros con la intranet o los canales internos establecidos y publicar documentos, estrategias o datos corporativos que pueden ser accesibles, e incluso fácilmente copiados, por terceros no autorizados. A su vez, este empleado también podría publicar opiniones o hacer comentarios de tipo eminentemente personal que un lector malintencionado podría hacer pasar por oficiales. En este mismo contexto y estrechamente relacionado, la AEPD se ha hecho eco en diversas ocasiones del peligro que pueden representar los grupos de empleados y los comentarios vertidos en ellos en situaciones de acoso laboral, sexual y casos de discriminación.

Los límites de usos de redes sociales han de quedar claramente definidos en la política interna de la entidad. Si en la política se admiten este tipo de canales de comunicación, se está admitiendo un tratamiento del que será responsable la entidad y, por lo tanto, habrá de cumplir con los establecido en el RGPD y en el ENS.

"EN LA POLÍTICA DE INFORMACIÓN DE LA ENTIDAD HA DE QUEDAR CLARO, AL MENOS DESDE LA PERSPECTIVA DE PROTECCIÓN DE DATOS, LA PROHIBICIÓN DE REALIZAR EL TRATAMIENTO DE DATOS PERSONALES RELATIVOS A LA ACTIVIDAD DE LA ENTIDAD A TRAVÉS DE LOS PERFILES PERSONALES EN LAS REDES SOCIALES PARTICULARES DE LOS EMPLEADOS".

EMPLEADOS QUE PUBLICAN EN REDES SOCIALES DE FORMA INDIVIDUAL

También es bastante común que profesionales publiquen contenidos en redes sociales aportando su experiencia al conocimiento común. En algunas organizaciones es frecuente incluso que se promueva el uso de las redes sociales por los expertos de la entidad.

Sin embargo, que los empleados publiquen información profesional puede infringir los principios de protección de datos, cuando se incluye información personal y se carece de legitimación.

Por ello, en la Política de Información de la entidad ha de quedar claro, al menos desde la perspectiva de protección de datos, la prohibición de realizar el tratamiento de datos personales relativos a la actividad de la entidad a través de los perfiles personales en las redes sociales particulares de los empleados.

EL USO DE REDES SOCIALES PARA LA OFERTA DE SERVICIOS A LOS CIUDADANOS

El 'Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos', establece como canal de asistencia para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito competencial, entre otros, el de las redes sociales.

Ahora bien, **cuando una Administración Pública decida ofrecer información o servicios a los ciudadanos a través de una red social, no puede obligar al administrado a contar con perfiles en la misma**, en la medida en que estas redes realicen tratamientos adicionales de datos basados en el consentimiento del usuario. Por ejemplo, realizar iniciativas de participación ciudadana únicamente a través de redes sociales obliga a aquellos sujetos que quieran tener influencia en dicha iniciativa a consentir en el tratamiento de un tercero y, en consecuencia, a otorgar un consentimiento que podría no cumplir los requisitos del RGPD.

"EL SERVICIO PROPORCIONADO A TRAVÉS DE LA RED SOCIAL DEBERÁ CUMPLIR CON TODAS LAS OBLIGACIONES ESTABLECIDAS EN EL RGPD, ENTRE ELLAS EL DEBER DE INFORMAR".

DEBER DE INFORMAR

El servicio proporcionado a través de la red social deberá cumplir con todas las obligaciones establecidas en el RGPD, entre ellas el deber de informar. Esta obligación podría implementarse en un post fijado al inicio de la cuenta de forma que el usuario pueda acceder fácilmente y que proporcionase la política de privacidad o un enlace a la misma.

LEGITIMACIÓN

El tratamiento de los datos por parte de las redes en la que los usuarios disponen de cuenta se basará, en general, en aquellos necesarios para la ejecución del contrato de servicio o en el consentimiento prestado. Hay que distinguir dichas causas de legitimación de las de aquellos tratamientos de los datos de los ciudadanos realizados por las Administraciones Públicas con perfil en las redes sociales derivados de la interacción con las personas a raíz de la información proporcionada por la Administración a través de su cuenta oficial y cuya legitimación para ser tratados por la Administración estaría basada en el cumplimiento de una misión realizada en interés público o en el ejercicio de los poderes públicos conferidos.

COOKIES

El tratamiento de datos realizado por la red social podría incurrir en la recogida de un volumen mayor de datos personales del ciudadano de los necesarios por parte de la Administración Pública en la gestión de su perfil oficial o de datos adicionales que no tengan ninguna relación con dicha gestión. El rol que la Administración Pública y la red social desempeñan respecto al tratamiento de los datos personales recogidos podría cambiar a corresponsables dependiendo de si la Administración Pública no es diligente para conocer dicha circunstancia, o, conociéndolos, tiene opciones para configurar o limitar el tratamiento que realiza la red social y no hace uso de ellos, o permite activamente que se produzca el tratamiento. Por ejemplo, en caso de los widgets a las redes sociales incluidas en los portales de las Administraciones, antes de permitir el uso de cookies por dichos recursos, es necesario que las Administraciones recaben el consentimiento previo del visitante de sus

páginas, manteniendo los widgets deshabilitados hasta su obtención.

"LA ENTIDAD HA DE DISPONER DE UNA POLÍTICA DE COMUNICACIÓN EN REDES SOCIALES QUE REFLEJE ASPECTOS DE LA POLÍTICA DE PROTECCIÓN DE DATOS DE LA ENTIDAD".

POLÍTICA DE COMUNICACIÓN EN REDES SOCIALES

La entidad ha de disponer de una política de comunicación en redes sociales que refleje aspectos de la Política de Protección de Datos de la entidad como son:

- Una responsabilidad clara y embebida de forma eficiente en la cadena de responsabilidades de la entidad, de manera que la comunicación por la red o redes sociales esté bien alineada con el resto de la política de comunicación institucional.

- Un documento informativo para los empleados públicos donde se indique qué pueden hacer y qué no en la red social de la Administración. Si se parte de la base de que las redes sociales son un apoyo o complemento a una página web y una sede oficial, es más fácil limitar el servicio y evitar riesgos.

- Una formación adecuada a las personas encargadas de publicar contenidos y atender a comentarios y cuestiones.

PERFILADO DE LOS USUARIOS

Las redes sociales pueden ser un medio para que las Administraciones conozcan datos estadísticos de sus usuarios, a través de la información que proporciona la propia plataforma. Esto podría realizar un perfilado de los usuarios, de sus intereses y de sus tendencias de navegación. En la medida en la que involucran tratamientos de datos personales, además de estar legitimado, especialmente cuando de la navegación se pueden inferir categorías especiales de datos, se debe proporcionar información de dichos tratamientos de conformidad con los artículos 13 y 14 del RGPD.

"EL CONTENIDO DE TERCEROS, INSERTADO COMO ANUNCIOS O DE OTRA FORMA, PUEDE LLEVAR A ENGAÑO A LOS USUARIOS Y HACER CREER A ESTOS QUE SON ENLACES QUE PERTENECEN A SERVICIOS DE LA ADMINISTRACIÓN PÚBLICA QUE RECABAN DATOS PERSONALES, POR LO QUE DICHOS CONTENIDOS HAN DE ESTAR BAJO SUPERVISIÓN O CONTROLAR EL TIPO DE CONTENIDOS QUE SE PUEDE OFRECER, EN PARTICULAR, CONTENIDOS RELACIONADOS CON IDEOLOGÍAS Y CREENCIAS DE CUALQUIER ÍNDOLE".

RIESGOS PARA LOS DERECHOS Y LIBERTADES DE LOS CIUDADANOS ASOCIADOS A LAS REDES SOCIALES

Una vez que se ha diseñado un tratamiento a través de redes sociales que cumpla con los requisitos establecidos en el RGPD, es necesario analizar los riesgos que para los derechos y libertades de los ciudadanos se pueden originar, con el fin de llevar a cabo la gestión adecuada de los mismos.

Algunos de estos riesgos son:

- Que se produzcan errores en la aplicación de las políticas de comunicación a través de redes sociales que desvelen datos de carácter personal de forma indeseada tanto de los administrados como de los propios empleados públicos (publicación de CSV, metadatos...). Para reducir el riesgo es necesaria la definición de una política interna clara y bien conocida por el personal sobre las implicaciones y consecuencias de la participación en redes sociales.

- Las cuentas abiertas en una red social por una Administración Pública pueden verse comprometidas y por tanto se puede infiltrar contenido en ellas con el propósito de recabar datos de carácter personal. Esto tiene que ser tenido en cuenta a la hora de gestionar los procesos de asignación y renovación de claves de acceso.

- Por otro lado, el contenido de terceros, insertado como anuncios o de otra forma, puede llevar a engaño a los usuarios y hacer creer a estos que son enlaces que pertenecen a servicios de la Administración Pública que recaban datos personales, por lo que dichos contenidos han de estar bajo supervisión o controlar el tipo de contenidos que se puede ofrecer, en particular, contenidos relacionados con ideologías y creencias de cualquier índole.

"EN CASO DE QUE, PARA EL ACCESO A LOS CONTENIDOS DE LA RED SOCIAL, SE REQUIERA INICIAR UNA SESIÓN POR PARTE DEL ADMINISTRADO, LA ADMINISTRACIÓN PÚBLICA HA DE EVALUAR LAS GARANTÍAS DE PRIVACIDAD, INCLUYENDO LAS MEDIDAS DE SEGURIDAD ORIENTADAS A LA PRIVACIDAD QUE PROPORCIONA DICHA RED, ESPECIALMENTE LA POLÍTICA DE CREACIÓN DE USUARIOS Y CONTRASEÑAS".

- En el caso de que se proporcionen espacios a los administrados para subir sus propios contenidos, se recomienda evitar que la publicación de dichos contenidos se realice sin supervisión para evitar la divulgación de información personal de terceros sin su consentimiento, en particular, contenido sensible o cualquier conducta que tuviera implícitos actos de violencia digital.

- En caso de que, para el acceso a los contenidos de la red social, se requiera iniciar una sesión por parte del administrado, la Administración Pública ha de evaluar las garantías de privacidad, incluyendo las medidas de seguridad orientadas a la privacidad que proporciona dicha red, especialmente la política de creación de usuarios y contraseñas. Este análisis ha de realizarse en interés de los ciudadanos, pero también en la de los gestores del espacio pudiendo un atacante suplantar a los publicadores.

- De cara a las responsabilidades asumidas por las Administraciones y relacionado con las tecnologías de seguimiento (cookies), es preferible que en el sitio web de la Administración, o en las *newsletters* que en su caso se distribuyan, se incluyan enlaces estáticos al perfil oficial en la red social, frente al empleo de widgets embebidos en el contenido.

- Las técnicas actuales no siempre permiten determinar con total efectividad que el usuario pueda ser un menor de edad. Habrá que evaluar el riesgo que esto supone con relación al tipo de contenidos que se están ofreciendo a través de la red y, en función de este riesgo, establecer procedimientos adicionales para la comprobación más precisa de la edad de los usuarios.

MATERIAL COMPLEMENTARIO

- Tecnologías y Protección de Datos en las AA.PP (AEPD). Consulta en este enlace.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. Consulta en este enlace.
- Guía de Comunicación Digital para la Administración General del Estado. Fascículo 8. Consulta en este enlace.
- 'Medidas de seguridad en Facebook' (AEPD). Consulta en este enlace.
- Buenas prácticas en Redes Sociales. (CCN-CERT). Consulta este enlace.
- Protege tu perfil corporativo en redes sociales con estos consejos del CCN (CCN-CERT). Consulta este enlace.

NOTICIAS

- **Nuevo formulario de notificación de brechas de datos personales.**

  La Agencia Española de Protección de Datos ha actualizado el formulario habilitado para que los responsables de los tratamientos de datos personales cumplan con su obligación de notificar las brechas que se hayan producido. Este nuevo sistema simplifica la notificación de brechas de datos personales guiando a los responsables a través de preguntas concretas, de forma que los responsables conozcan los puntos que deben abordar en la misma.

  Consulta más detalles en este enlace.

- **La AEPD publica una nueva guía para gestionar el riesgo de los tratamientos de datos personales y realizar evaluaciones de impacto.**

  La Agencia Española de Protección de Datos ha publicado la guía 'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales', un documento que incorpora la experiencia acumulada en la aplicación de la gestión del riesgo en el ámbito de la protección de datos desde la aplicación del Reglamento General de Protección de Datos (RGPD) y añade las interpretaciones de la AEPD, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos.

  El documento, dirigido a responsables, encargados de tratamientos y delegados de protección de datos (DPD), ofrece una visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

  Consulta la Guía en este enlace.