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 10 | Abril 2021

EL CONSENTIMIENTO

Í N D I C E

EL CONSENTIMIENTO

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: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"EN EL TEXTO DEL RGPD, EL CONSENTIMIENTO SE RECOGE COMO UNA DE LAS SEIS CAUSAS DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES, SIN OSTENTAR MAYOR O MENOR IMPORTANCIA QUE OTRAS".

INTRODUCCIÓN

La reforma operada por el Reglamento General de Protección de Datos (RGPD) respecto del régimen contenido en la Ley Orgánica 15/1999 exige un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del "principio de consentimiento" el eje central del derecho a la protección de datos. Si bien la derogada Ley Orgánica y el actual Reglamento no difieren excesivamente en lo que respecta a la enumeración de las causas legitimadoras del tratamiento, se produce una modificación relevante en el modo en que dichas causas aparecen recogidas por los textos aplicables: así, mientras del tenor de la Ley Orgánica 15/1999 parecía deducirse que la regla básica de legitimación era, con carácter general, el consentimiento, resultando las restantes causas legitimadoras excepcionales, en el texto del RGPD el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento, sin ostentar mayor o menor importancia que las restantes que se enumeran.

A mayor abundamiento, el propio RGPD pone de manifiesto que el consentimiento del interesado no debe constituir la base legal del tratamiento en determinados supuestos. Por ejemplo, cuando el interesado no goza de verdadera o libre elección, cuando no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno, o en aquellos casos en los que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública.

En el presente cuaderno, analizaremos cómo se define este consentimiento por el legislador europeo y el español, las condiciones para su validez, así como su aplicabilidad en el ámbito del sector público. Del mismo modo, hablaremos de las formas de obtener el consentimiento de los interesados y de la posibilidad que estos tienen de revocar el consentimiento prestado. Por último, abordaremos la cuestión relativa al consentimiento para el tratamiento de datos de menores.

"HABRÍA DE EXAMINARSE CASO POR CASO LA APLICABILIDAD DEL CONSENTIMIENTO EN EL ÁMBITO DE LA ADMINISTRACIÓN PÚBLICA, PUES EL CONSENTIMIENTO OTORGADO POR LOS INTERESADOS A LA ADMINISTRACIÓN PODRÍA NO CONSIDERARSE OTORGADO LIBREMENTE EN DETERMINADAS CIRCUNSTANCIAS".

APLICABILIDAD Y CONDICIONES PARA SU VALIDEZ

De conformidad con el artículo 4.11 RGPD – y que recoge, literalmente, el artículo 6.1 LOPDGDD –, se entenderá por:

> ***«Consentimiento del interesado»:*** *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.*

«LIBRE»

Atendiendo al Considerando 42 RGPD: "*El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".*

El Considerando 43 RGPD, por su parte, nos dice que el consentimiento no será válido cuando: *"exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular"*

Por lo que, yendo al máximo rigor, habría de examinarse caso por caso la aplicabilidad de esta condición de licitud en el ámbito de la Administración Pública, pues el consentimiento otorgado por los interesados a la Administración podría no considerarse dado libremente en determinadas circunstancias.

A este respecto, el Grupo de Trabajo del Artículo 29 (GT29) considera que, sin perjuicio de que haya otras bases jurídicas más adecuadas para el tratamiento de datos por las autoridades públicas, el uso del consentimiento no queda totalmente excluido en virtud del marco jurídico del RGPD. En concreto, nos proporciona algunos ejemplos que muestran que el consentimiento puede ser adecuado en determinadas circunstancias:

"SIN PERJUICIO DE QUE HAYA OTRAS BASES JURÍDICAS MÁS ADECUADAS PARA EL TRATAMIENTO DE DATOS POR LAS AUTORIDADES PÚBLICAS, EL USO DEL CONSENTIMIENTO NO QUEDA TOTALMENTE EXCLUIDO EN VIRTUD DEL MARCO JURÍDICO DEL RGPD".

Ejemplo 1. *Un municipio está planificando obras de mantenimiento de carreteras. Dado que dichas obras pueden perturbar el tráfico durante un periodo largo de tiempo, el municipio ofrece a sus ciudadanos la oportunidad de suscribirse a una lista de correo electrónico con el fin de recibir información actualizada sobre el avance de las obras y sobre los retrasos previstos. El municipio deja claro que no existe la obligación de participar y pide el consentimiento para utilizar las direcciones de correo electrónico para este (único) fin. Los ciudadanos que no dan su consentimiento no se ven privados de ningún servicio básico del municipio o del ejercicio de ningún derecho, por ello tienen la capacidad de dar o negar libremente el consentimiento a este uso de los datos. La información sobre las obras estará también disponible en el sitio web del municipio.*

En este mismo sentido se pronunció la AEPD en la Resolución R/03041/2017, en la que recuerda al Ayuntamiento denunciado la exigencia de contar, no sólo con el consentimiento previo e inequívoco de los titulares afectados para incluir sus datos de carácter personal en grupos de WhatsApp o de cualquier otra aplicación de mensajería instantánea que ofrezca un servicio de comunicación electrónica grupal semejante, sino también de que dicho uso de datos personales responda a las finalidades concretas para las que se obtuvieron y fue autorizado su tratamiento.

Ejemplo 2. *Una escuela pública pide a sus alumnos el consentimiento para utilizar sus fotografías en una revista escolar impresa. El consentimiento en estas situaciones sería una elección real siempre que no se negara a los alumnos la educación u otros servicios y ellos pudieran negarse al uso de dichas fotografías sin sufrir ningún perjuicio.*

También la AEPD, en su 'Guía Sectorial de Protección de Datos y Administración Local' nos ofrece algunos ejemplos en los que el consentimiento legitimaría el tratamiento de los datos personales por parte de la Administración:

"PARA LA APLICACIÓN DEL CONSENTIMIENTO COMO BASE DE LEGITIMACIÓN EN LA ADMINISTRACIÓN PÚBLICA, ES RECOMENDABLE: VALORAR SI LOS TRATAMIENTOS AFECTADOS PUEDEN APOYARSE EN OTRA BASE LEGAL, Y VALORAR SI EL CONSENTIMIENTO FACILITADO POR EL PARTICULAR A LA ADMINISTRACIÓN SE PODRÍA ENTENDER DADO LIBREMENTE, TENIENDO EN CUENTA LAS CIRCUNSTANCIAS DE DICHA SITUACIÓN PARTICULAR".

- La suscripción a través de un servicio ofrecido por un Ayuntamiento en su página web para recibir comunicaciones referidas a las actividades culturales.

- La inscripción en una bolsa de trabajo.

En definitiva, para la aplicación del consentimiento como base de legitimación en la Administración Pública, es recomendable:

- Valorar si los tratamientos afectados pueden apoyarse en otra base legal.

- Valorar si el consentimiento facilitado por el particular a la Administración se podría entender dado libremente, teniendo en cuenta las circunstancias de dicha situación particular.

«ESPECÍFICA»

Esto implica que se consiente o acepte en concreto un tratamiento/s y/o cesión de dato/s. Para ello, debe haberse ofrecido al interesado la posibilidad de elegir las finalidades que consiente y las que no, sin obligarle a aceptarlas de forma conjunta.

«INFORMADA»

La declaración debe ir ligada al derecho de información del interesado. Esto es, se ha de informar acerca de qué datos se tratarán, cómo, para qué fines o usos, a quien/es podrían ser comunicados, y el resto de información señalada en los artículos 13 y 14 RGPD.

«INEQUÍVOCA»

Debe resultar evidente que el interesado ha dado su consentimiento a una operación concreta de tratamiento de datos. No caben formas tácitas, presuntas, negativas o dobles negaciones para recabar el consentimiento.

"LA DECLARACIÓN DE CONSENTIMIENTO PODRÍA INCLUIR: MARCAR UNA CASILLA DE UN SITIO WEB EN INTERNET, ESCOGER PARÁMETROS TÉCNICOS PARA LA UTILIZACIÓN DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN O CUALQUIER OTRA DECLARACIÓN O CONDUCTA QUE INDIQUE CLARAMENTE EN ESTE CONTEXTO QUE EL INTERESADO ACEPTA LA PROPUESTA DE TRATAMIENTO DE SUS DATOS PERSONALES".

FORMAS DE OBTENER EL CONSENTIMIENTO

Resulta de interés destacar la inclusión, por parte del RGPD, de las formas en las que puede obtenerse el consentimiento:

MEDIANTE UNA «DECLARACIÓN»

A los efectos de saber qué entendemos por esta «declaración», atenderemos al Considerando 32 RGPD, que nos indica que puede ser:

Por escrito, inclusive por medios electrónicos. - El propio Considerando indica en este sentido, que la declaración:

- Podría incluir marcar una casilla de un sitio web en internet.
- Escoger parámetros técnicos para la utilización de servicios de la sociedad de la información.
- Cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

El artículo 7.2 RGPD establece que, si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento debe presentar:

- De tal forma que se distinga claramente de los demás asuntos.
- De forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
- No será vinculante ninguna parte de la declaración que constituya infracción del RGPD.

Verbal. - Aunque se admite la validez de este, plantea un gran problema en cuanto a su eficacia jurídica, ya que es complicado probar su existencia en caso de incumplimiento. Y es que, "*Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales".* (Artículo 7.1 RGPD). Por esto, es importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo.

"NO DEBEN CONSTITUIR CONSENTIMIENTO: EL SILENCIO, LAS CASILLAS YA MARCADAS O LA INACCIÓN".

MEDIANTE UNA «CLARA ACCIÓN AFIRMATIVA»

Para saber qué hemos de entender por «clara acción afirmativa», el Considerando 32 RGPD nos señala, a *sensu contrario,* que NO deben constituir consentimiento:

- El silencio
- Las casillas ya marcadas
- La inacción

Por tanto, NO es admitido como válido el consentimiento por omisión o tácito. A estos efectos, supone inactividad del interesado, ya sea por silencio o por falta de negativa u oposición.

REVOCACIÓN DEL CONSENTIMIENTO

De conformidad con el artículo 7.3 RGPD *"El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo",* por lo que:

- La retirada del consentimiento no tiene efectos retroactivos. De este modo, el tratamiento de datos personales que se hubiera basado jurídicamente en el consentimiento del interesado, en el caso de que fuera retirado, no surtirá efectos al tratamiento de los datos que se hubiera hecho hasta el día en que se manifiesta la revocación.
- Al momento de obtener el consentimiento, el interesado debe ser informado de que después («en cualquier momento») tendrá la oportunidad de retirar o revocar dicho consentimiento.
- La regla general para la revocación es escueta, pero clara y contundente: *"Será tan fácil retirar el consentimiento como darlo".* De modo que, no han de adoptarse formulas, mecanismos o medios que disuadan, limiten o impidan al interesado retirar o revocar libremente el consentimiento.

EL CONSENTIMIENTO PARA TRATAR DATOS PERSONALES DE MENORES

"EL CONSENTIMIENTO PARA LA UTILIZACIÓN DE LOS DATOS PERSONALES DE MENORES DE 14 AÑOS SE DEBE OTORGAR POR SUS PADRES O TUTORES LEGALES".

MENORES DE 14 AÑOS

El consentimiento para la utilización de sus datos personales se debe otorgar por sus padres o tutores legales (Art. 7.1 LOPDGDD). El responsable del tratamiento hará esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. (Art. 8.2 RGPD).

Si bien el RGPD no incluye orientación sobre cómo verificar el consentimiento del titular de la patria potestad o tutela, el GT29, en sus 'Directrices sobre el consentimiento del RGPD', recomienda adoptar un enfoque proporcionado de acuerdo con el principio de minimización de datos, que puede centrarse en obtener una cantidad limitada de información, por ejemplo, los datos de contacto de un padre o tutor. Apunta que lo razonable, en relación con la verificación de que una persona que da su consentimiento en nombre de un niño sea el titular de la patria potestad o la tutela, puede depender de los riesgos inherentes al tratamiento, así como de la tecnología disponible. En casos de bajo riesgo, entiende que la verificación de la patria potestad o la tutela por correo electrónico puede ser suficiente. Por el contrario, en casos en los que el riesgo es elevado, entiende adecuado pedir más pruebas.

En cuanto a la verificación de la edad del menor, si los usuarios declaran que superan la edad de consentimiento, aunque el RGPD no indica explícitamente la necesidad de adoptar todas las medidas razonables para verificar la edad, el GT29 señala en las Directrices antes mencionadas que el responsable podrá llevar a cabo las comprobaciones necesarias para verificar que dicha declaración es cierta. Entiende que está implícito en el Reglamento ya que, si un niño da su consentimiento a pesar de no tener edad para prestar un consentimiento válido en su propio nombre, el tratamiento de los datos no será lícito.

"EL RESPONSABLE DEL TRATAMIENTO DEBE HACER ESFUERZOS RAZONABLES PARA VERIFICAR QUE EL CONSENTIMIENTO FUE OTORGADO O AUTORIZADO POR EL TITULAR DE LA PATRIA POTESTAD O TUTELA SOBRE EL NIÑO, TENIENDO EN CUENTA LA TECNOLOGÍA DISPONIBLE".

Al igual que para la verificación del consentimiento dado por el padre/madre/tutor, la verificación de la edad no debe conducir a un tratamiento excesivo de datos, por lo que el mecanismo elegido para verificar la edad del interesado debe conllevar una evaluación del riesgo del tratamiento propuesto. En algunas situaciones de bajo riesgo, el GT29 entiende adecuado solicitar el año de nacimiento o rellenar un formulario en el que declaren que son (o no son) menores, y en caso de duda, considerar si se requieren otras comprobaciones.

Como ya señalamos en el cuaderno del mes pasado, en la AEPD existen numerosos procedimientos sancionadores que se han llevado a cabo con el objetivo de verificar la edad de los menores. En el PS/00281/2007, el formulario incluía un campo para indicar la fecha de nacimiento. En este caso se registró un menor de 9 años y completó parcialmente el campo "fecha de nacimiento", lo que provocó que el sistema asignara al usuario la edad de 1911 años. Como resultado, el niño recibió una promoción comercial de una tarjeta de crédito de una institución financiera. La AEPD observó una falta de diligencia del responsable y señaló que debería haber tomado las medidas adecuadas para evitar el registro y, sobre todo, el posterior tratamiento de los datos de menores. Además, la anomalía producida en cuanto a la edad del usuario registrado no dio lugar a controles adicionales sobre una circunstancia que afectaba al único elemento orientado a intentar verificar efectivamente la edad del usuario.

Recordemos también el PS/00468/2009, en el que la AEPD sancionó un sitio web dirigido a niños y jóvenes en el que se ofrecían servicios de chat y juegos, entre otros, por la recogida de datos de un menor de 14 años sin el consentimiento paterno requerido. En este caso, el sitio web sólo solicitaba registrar una dirección de correo electrónico, nombre de usuario y contraseña, además de otros datos como fecha de nacimiento sólo opcionalmente. En la política de protección de datos de dicho portal se estableció que, en el caso de usuario menor de 14 años, manifestaba que contaba con el consentimiento previo de sus representantes legales y que había cumplimentado el formulario bajo su supervisión. La AEPD no consideró que esta cláusula fuera suficiente para la verificación de la edad o el consentimiento de los padres, indicando que la mera

“AL IGUAL QUE PARA LA VERIFICACIÓN DEL CONSENTIMIENTO PARENTAL, SEGÚN EL CASO CONCRETO Y EL RIESGO INHERENTE AL TRATAMIENTO, EL RESPONSABLE DEBERÁ VALORAR SI UTILIZA MECANISMOS MÁS SENCILLOS O MÁS COMPLEJOS PARA VERIFICAR LA EDAD DEL INTERESADO”.

cuestión de la edad no era considerada como un método fiable de verificación en un formulario web, especialmente cuando las respuestas ya están establecidas por defecto como, por ejemplo, si solo se puede poner que el usuario es mayor de catorce años para poder continuar, o cuando se incorporen cláusulas o políticas por las cuales el usuario simplemente declara ser mayor de edad sin darle la opción de ingresar la edad específica o haber obtenido el consentimiento de los padres en el caso de ser menor de 14 años.

En definitiva, al igual que para la verificación del consentimiento parental, según el caso concreto y el riesgo inherente al tratamiento, el responsable deberá valorar si utiliza mecanismos más sencillos o más complejos para verificar la edad del interesado. En los supuestos de menor riesgo, la verificación podría realizarse solicitando determinados datos o mediante "preguntas de control" que, en principio, no podría responder razonablemente un menor, que podrían complementarse con métodos como impedir al usuario volver una vez se le negó el acceso por no alcanzar la edad suficiente. Y en supuestos de mayor riesgo, podría recurrirse a sistemas de verificación o identificación a través de documentos de identidad. Ésta fue la solución elegida por la ya desaparecida red social Tuenti, que en 2009 implementó un proceso de depuración de los perfiles de menores de 14 años, de modo que cuando advertía que un perfil podía pertenecer a un menor de 14 años, le solicitaba proporcionar una fotocopia de su DNI o pasaporte en menos de 92 horas. En caso de no recibir respuesta, el perfil del usuario se eliminaba.

MENORES ENTRE 14 Y 18 AÑOS

Podrán otorgar el consentimiento para la utilización de sus datos personales por sí mismos, salvo que una norma específica exija la asistencia de los padres o tutores (art. 7.1 LOPDGDD).

MATERIAL COMPLEMENTARIO

- Guía: 'Protección de Datos y Administración Local' (AEPD). Consulta la Guía en este enlace.
- 'Directrices sobre el consentimiento en el sentido del RGPD' (GT29). Consulta las directrices en este enlace.
- Infografía sobre el consentimiento de menores (AEPD). Consulta la infografía en este enlace.
- Resolución R/03041/2017 (AEPD). Consulta la Resolución en este enlace.
- Resolución R/00893/2010 (AEPD). Consulta la Resolución en este enlace.

NOTICIAS

- **Durante el mes de febrero de 2021, se ha experimentado un incremento sustancial en las notificaciones de brechas de seguridad recibidas por la Agencia Española de Protección de Datos (AEPD).**

  Con carácter mensual, la AEPD emite un informe resumiendo las características principales de las notificaciones de brechas de seguridad recibidas en la Agencia Española de Protección de Datos (AEPD), en virtud del artículo 33 del RGPD.

  En el último informe publicado, el del mes de febrero, se aprecia un incremento sustancial en las notificaciones recibidas respecto a meses anteriores. Un incidente de seguridad de tipo *ransomware* en un encargado de tratamiento que ha causado brechas de seguridad con consecuencias diversas en varios responsables habría producido este incremento. Consulta el Informe de notificaciones de brechas de seguridad d ela AEPD del mes de febrero en este enlace.

- **La Autoridad Catalana de Protección de Datos (APDCAT) emite un Dictamen en relación con una consulta sobre la identificación de las personas interesadas que ostentan la condición de víctima de violencia de género en las diferentes publicaciones de los procedimientos selectivos de personal.**

  Se presenta ante la Autoridad Catalana de Protección de Datos (APDCAT) un escrito en el cual se solicita que la Autoridad emita un dictamen sobre la identificación de las personas interesadas que ostentan la condición de víctima de violencia de género en las diferentes publicaciones de los procedimientos selectivos de personal. Señala la APDCAT al respecto que, las personas aspirantes que acrediten tal condición tienen derecho a la protección de sus datos personales en las diferentes publicaciones de los procedimientos de selección. Para hacer efectiva esta protección y mientras no se apruebe el protocolo en que hace mención el apartado 2.ª de la Disposición adicional séptima del LOPDGDD, la identificación de estas personas mediante la asignación del código ID a que se refiere la consulta resultaría adecuada a la normativa de protección de datos. Consulta el Dictamen en este enlace.