bizkaiko hirugarren sektorearen behatokia
observatorio del tercer sector de bizkaia
3s bizkaia .org

Kudeaketako laburra
Breve de gestión

2018ko otsaila
febrero 2018

La nueva normativa europea de protección de datos y las organizaciones del Tercer Sector Social

Contenidos

El próximo 25 de mayo comenzará a aplicarse el Reglamento General de Protección de Datos,[1] que es una normativa aprobada en el seno de la Unión Europea tras un periodo prolongado de intensos debates, con la finalidad de reforzar la protección de la privacidad e imponer la misma regulación a los diferentes países que integran la UE.

Esta norma entró en vigor el 25 de mayo de 2016, estableciéndose un periodo de transición de dos años, para que tanto los Estados de la Unión Europea como las empresas y entidades públicas y privadas que tratan datos pudieran adaptar sus procedimientos de trabajo al nuevo Reglamento. **Ese periodo está a punto de finalizar y el Reglamento será de plena aplicación.**

Hasta ahora, la normativa de referencia era la LOPD o, lo que es lo mismo, la Ley Orgánica de Protección de Datos del año 1999, basada en la Directiva comunitaria 95/46, que ha venido regulando a nivel estatal el derecho fundamental a la protección de datos personales durante casi 20 años.

De ahora en adelante, el marco normativo obligatorio será el Reglamento Europeo, común para todos los estados miembros. Sin embargo, es posible que sigamos oyendo hablar de la LOPD, ya que, aunque la del año 1999 quedará derogada, se está tramitando en vía parlamentaria una nueva Ley Orgánica de Protección de Datos que complementará y clarificará algunas cuestiones del Reglamento.

[1] El nombre oficial es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
Para facilitar la lectura, nos referiremos a dicha norma como Reglamento General de Protección de Datos, RGPD, el Reglamento Europeo, o, simplemente, el Reglamento.

1. ¿También nos afecta a las entidades del tercer sector?

Indudablemente, sí. Las entidades del tercer sector tratamos datos personales de diferentes colectivos. Fundamentalmente, manejamos datos tanto de las personas usuarias o destinatarias de los servicios y actividades que ofrecemos, como del equipo de personas trabajadoras y voluntarias. Además, gestionamos datos de personas socias, donantes, y datos de contacto en general.

Tratar datos personales no implica sólo conocer datos íntimos o más sensibles, sino también cualquier tipo de información relacionada con una persona. Por tanto, cuando conocemos el nombre y apellidos, el DNI, el número de cuenta, o incluso la dirección de correo electrónico de una persona estamos tratando sus datos y nos afecta la normativa de protección de datos y las obligaciones que esta impone.

"cuando conocemos el nombre y apellidos, el DNI, el número de cuenta, o incluso la dirección de correo electrónico de una persona estamos tratando sus datos y nos afecta la normativa de protección de datos y las obligaciones que esta impone."

Así, cuando hacemos envíos informativos por correo electrónico o por aplicaciones móviles al listado de personas destinatarias habitual, debemos hacerlo con las garantías adecuadas y respetando la normativa de privacidad.

Por otra parte, no hay que olvidar que también una fotografía, así como una grabación de video o audio está sujeta a esta normativa, siempre que se pueda identificar a quien aparece.

Es evidente que no todos los datos personales son iguales, ni tampoco la finalidad para la que se utilizan. Es posible que nos agrade aparecer en una foto del periódico local por haber ganado un concurso. Sin embargo, es probable que no nos guste tanto que se revele información que consideramos más personal, por ejemplo, aparecer en un listado de morosos.

Hay algunos tipos de datos que se consideran especialmente sensibles y su tratamiento requerirá unas garantías mayores (ideología, religión, salud, vida sexual....). Como novedad, el RGPD define los datos genéticos y los biométricos, como puede ser el uso de la huella dactilar para desbloquear el teléfono móvil.

Las entidades del tercer sector social tratamos datos personales continuamente y por eso es tan importante que conozcamos qué debemos hacer.

¿Cómo debemos recoger la información que necesitamos para poder prestar un servicio determinado? ¿De verdad necesitamos tanta información? ¿Cuánto tiempo podemos conservar los datos? ¿Dónde los tenemos que guardar? ¿Podemos intercambiar los datos de las personas usuarias entre las entidades?

La normativa de protección de datos resuelve estos interrogantes y muchos otros, obligándonos a gestionar la información personal con unas garantías adecuadas, que protejan la privacidad.

El Reglamento General de Protección de Datos afianza los principios básicos de protección de datos que recogía la Ley Orgánica de Protección de Datos, los completa, e incorpora algunas novedades, evolucionando a un modelo más garantista.

2. ¿Cuáles son los cambios más importantes que implica el reglamento?

El nuevo Reglamento europeo supone un cambio significativo en el modelo de protección de datos que imponía la LOPD, ya que evoluciona de un esquema de cumplimiento pasivo a un modelo basado en la responsabilidad proactiva.

Se parte del cumplimiento de unos requisitos estandarizados, es decir, unas obligaciones claras y determinadas, impuestas por la LOPD, y se pasa a un modelo más abierto, que conjuga la prevención con la implantación efectiva de las medidas más apropiadas para cada organización, siempre con la finalidad de proteger los datos personales y, todo ello, en el marco que establece el Reglamento.

Ya no basta decir: "sí, en mi entidad hacemos lo que obliga la normativa de protección de datos" sólo por cumplir el expediente.

Con el RGPD se establece un cambio de enfoque, se busca la protección de datos como compromiso, adoptando protocolos y medidas que razonablemente aseguren que se cumple con la privacidad desde el momento inicial en que se está gestando un producto o servicio determinado. Con el nuevo modelo, se exige una actitud consciente, diligente y proactiva por parte de las entidades en cada uno de los tratamientos de datos que llevemos a cabo.

Esta responsabilidad debe ser tanto activa como demostrable. Por tanto, además de cumplir con las exigencias normativas, debemos demostrar que hemos implementado las medidas adecuadas para garantizar la privacidad y que los datos se tratan de conformidad con el Reglamento.

Por otra parte, el nuevo modelo también es un avance para la ciudadanía, ya que el Reglamento Europeo no sólo se aplica a las empresas establecidas en Europa sino a todas las que se dirijan a la ciudadanía europea, incluyendo también a las grandes multinacionales que ofrecen servicios de redes sociales, aplicaciones móviles o mensajería electrónica, en relación con las y los consumidores europeos.

3. ¿Qué obligaciones principales establece el reglamento?

"La piedra angular de la protección de datos es el poder de control de cada cual sobre sus datos personales, lo que implica que cada persona tiene la potestad de decidir qué información sobre sí misma quiere facilitar, conociendo a quién se la da y para qué se va a utilizar."

Información y consentimiento

La piedra angular de la protección de datos es el poder de control de cada cual sobre sus datos personales, lo que implica que cada persona tiene la potestad de decidir qué información sobre sí misma quiere facilitar, conociendo a quién se la da y para qué se va a utilizar.

La capacidad de controlar los datos propios se refuerza con el nuevo Reglamento, endureciendo tanto la obligación de informar como la de solicitar el consentimiento y fortaleciendo el concepto de consentimiento informado, que se basa en que cada persona debe conocer qué es lo que se va a hacer con sus datos antes de decidir si los facilita o no.

Una novedad importante es que el Reglamento exige que la información sea concisa, transparente, inteligible y de fácil acceso, y que se explique con un lenguaje claro y sencillo. Se pretende terminar con las cláusulas informativas de protección de datos y avisos de privacidad farragosos y de difícil comprensión, y las que se limitan a "copiar y pegar".

Por tanto, las entidades tendremos que hacer un esfuerzo por informar de forma más amplia y también más clara, aumentando las cuestiones a comunicar y, al mismo tiempo, buscando fórmulas comprensibles fácilmente.

Otra de las grandes novedades es que, cuando la base de legitimación para tratar datos sea el consentimiento, será imprescindible que sea expreso. Ya no vale el consentimiento tácito ni las casillas pre-marcadas en las páginas web para aceptar las condiciones o las políticas de privacidad. El Reglamento establece que el consentimiento es una manifestación de voluntad inequívoca que debe basarse en una declaración o en una clara acción afirmativa.

Aunque la norma general es que para tratar datos personales antes hay que recabar el consentimiento previo, existen supuestos en los que se pueden tratar datos amparándose en otra base de legitimación permitida por el Reglamento.

Por ejemplo, se podrían tratar datos personales sin solicitar el consentimiento cuando se produce una urgencia sanitaria o existe una ley que nos obliga a notificar nuestros datos, como por ejemplo en la campaña anual de la Declaración de la Renta.

Contratos entre organización responsable y encargada

En ocasiones, las organizaciones contratamos los servicios de terceros que realicen labores especializadas, como por ejemplo: la gestión de los contratos y las nóminas, el envío de cartas, los servicios informáticos, etc.

A estos terceros que prestan un servicio se les facilitan datos personales para que puedan realizar las actividades contratadas y la normativa de protección de datos les denomina "*encargados"* del tratamiento de datos, manteniéndose la entidad que les contrata como responsable.

Es incluso más frecuente el supuesto inverso, es decir, que las entidades actuemos como encargadas frente a clientes para los que realizamos un servicio o frente a las administraciones públicas con las que cooperamos en la provisión de servicios de su responsabilidad.

Por tanto, al tratar datos tenemos que preguntarnos, en primer lugar, si somos "*responsables*" del tratamiento o "*encargadas*", ya que las obligaciones pueden variar.

Hay supuestos en que la respuesta es evidente. Sin embargo, otras veces, sobre todo cuando se tratan datos para la Administración Pública, la respuesta no siempre es tan clara como parece, y tenemos que fijarnos en lo que establece el contrato o convenio que regula la relación.

En todos estos supuestos, en los que existe una organización responsable y una encargada, es imprescindible que se firme un contrato o convenio escrito, con un contenido mínimo preestablecido en el Reglamento Europeo, ampliando las estipulaciones exigibles por la LOPD.

Una de las novedades del Reglamento más relevante para las entidades del tercer sector social es que la organización responsable tiene un deber de diligencia al elegir a la encargada y debe asegurarse de que le ofrezca garantías suficientes en el cumplimiento de la normativa de protección de datos.

Por tanto, las administraciones públicas con las que cooperamos en la provisión de servicios o las organizaciones "cliente" de las entidades deberán ser más rigurosas al controlar que respetamos dicha normativa y las entidades tendremos que demostrar su observancia.

Medidas de responsabilidad proactiva

Como se ha expuesto, una de las grandes innovaciones del Reglamento son las medidas de responsabilidad proactiva que las entidades y empresas tienen que adoptar. A continuación las enumeramos y comentamos muy brevemente:

Registro de actividades de tratamiento

La LOPD obligaba a las empresas y entidades a comunicar sus ficheros de datos personales a la Agencia de Protección de Datos. Muchas empresas y entidades creían erróneamente que cumpliendo con este requisito era suficiente para entender que estaban adaptadas a la normativa de protección de datos, lo que no era correcto.

"La LOPD obligaba a las empresas y entidades a comunicar sus ficheros de datos personales a la Agencia de Protección de Datos. Muchas empresas y entidades creían erróneamente que cumpliendo con este requisito era suficiente para entender que estaban adaptadas a la normativa de protección de datos, lo que no era correcto."

Esta exigencia de inscripción de ficheros desaparece con el Reglamento Europeo y se sustituye por la de contar con un registro de actividades interno actualizado, en el que se indiquen los diferentes tratamientos de datos que realiza una entidad.

Delegado o Delegada de Protección de Datos (DPD o DPO)

Es una nueva figura que va a resultar clave en la gestión de la privacidad, obligatoria en todas las Administraciones Públicas y, en muchos casos, en las entidades y empresas privadas.

Sus funciones, sus requisitos profesionales y su posición en la entidad están delimitadas en el Reglamento, con el fin último de garantizar el cumplimiento efectivo de la normativa de protección de datos.

Gestión de la seguridad

El Reglamento estipula que es necesario que se determine el nivel de riesgo para los derechos y libertades de las personas interesadas en relación con la privacidad, con la finalidad de decidir cuáles son las medidas a implementar. Se trata de evaluar y gestionar los riesgos, implantando las medidas de seguridad más adecuadas a los riesgos detectados, frente al modelo establecido por la LOPD, que indicaba las medidas de seguridad a llevar a cabo, en función del tipo de datos personales.

Privacidad desde el diseño y por defecto

En grandes líneas supone, que desde el inicio de un proyecto o servicio y a lo largo del proceso, hay que tener en cuenta la privacidad, implementando las medidas organizativas y técnicas más adecuadas para proteger los datos personales.

Evaluaciones de impacto sobre la privacidad

En algunos tratamientos de datos será necesario realizar evaluaciones de impacto con carácter previo a su puesta en marcha, para determinar los riesgos que podrían suponer respecto a la privacidad y poner en marcha las medidas necesarias para evitarlos o, al menos, minimizarlos.

Notificación de violaciones de seguridad

Cuando se produce una brecha de seguridad, el Reglamento establece la obligación de notificarlo a la Agencia de Protección de Datos, sin demora, y, a más tardar en 72 horas desde que se haya tenido constancia, y, en supuestos muy graves, también a las posibles personas afectadas.

Por otra parte, la organización encargada tiene obligación de notificar al responsable de tratamiento, sin dilación, todas las brechas de seguridad que ocurran.

Códigos de conducta y certificaciones

El RGPD promueve los códigos de conducta, que vienen a ser documentos redactados voluntariamente por una empresa o entidad, o por un grupo de ellas, en el que se exponen una serie de principios respecto a la protección de datos que se comprometen a cumplir.

Su finalidad es contribuir a la correcta aplicación de la normativa de protección de datos, teniendo en cuenta las características de los sectores de tratamiento y la idiosincrasia de las entidades firmantes.

Además, el Reglamento fomenta las certificaciones, que son mecanismos para acreditar el cumplimiento de las obligaciones y para garantizar que las entidades adheridas a un código de conducta, efectivamente lo cumplen.

4. ¿Qué ocurre si no cumples la normativa de protección de datos?

Autoridades de control

El Reglamento General de Protección de Datos establece que en cada uno de los estados miembros de la Unión Europea debe existir al menos una autoridad encargada de velar por la aplicación del Reglamento, que denomina autoridad de control, profundizando en su regulación y fomentando su cooperación.

En España, el modelo ya existente de la Agencia Española de Protección de Datos y las Agencias de Protección de Datos de Euskadi y Cataluña sigue funcionando y las agencias asumen el papel de autoridades de control en sus ámbitos de competencia.

Régimen sancionador

Con el nuevo modelo establecido en el Reglamento Europeo, se flexibiliza el régimen sancionador. Por un lado, se incorporan numerosos criterios de modulación para las multas, en función de las circunstancias de cada caso. Por otro lado, además de las multas económicas, se prevén acciones correctivas, que las autoridades de control pueden imponer junto a las multas o en su lugar, como pueden ser advertencias, órdenes de adaptación a tratamientos, limitaciones temporales o definitivas, etc.

Es importante tener en cuenta que las sanciones son aplicables tanto a las organizaciones responsables como a las encargadas y pueden llegar a ser de 10 millones de euros o el 2% del volumen de negocio, o de 20 Millones de euros o el 4% del volumen de negocio, en función del tipo de infracción.

Para profundizar

Inscríbete en la jornada que hemos organizado en Bilbao, Donostia-San Sebastián o Vitoria-Gasteiz el próximo mes de junio:

Accede a este video-resumen que recoge las ideas principales sobre el tema del breve:

Entra en la Agencia Española de Protección de Datos o la Agencia Vasca de Protección de Datos, en cuyos respectivos sitios web disponen de diferentes guías, documentos orientativos y herramientas, así como el Reglamento General de Protección de datos.

Agencia Española de Protección de datos

Agencia Vasca de Protección de Datos