LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO ASOCIATIVO

bolunta
boluntariotza eta gizarte-partaidetza
voluntariado y participación social
Bizkaia | edefundazioa | bbk

LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO ASOCIATIVO

1. ¿Qué es la protección de datos y cómo afecta a una asociación?

- Los datos personales son **cualquier información relativa a personas físicas identificadas o identificables** por ejemplo nombre, NIF, email, foto, etc.
- **La ley obliga a todo el mundo a proteger** el uso y archivo de datos de personas físicas vivas **siempre que no sean para un uso exclusivamente doméstico:** p.ej. fotos de mi hijo con sus amigos en las actividades extraescolares que no voy a compartir con nadie salvo mi familia, y por supuesto nunca en redes sociales.
- **Las asociaciones recogemos y archivamos datos personales de las personas** que vienen a nuestra asociación: personas socias, trabajadoras, voluntarias, colaboradoras, destinatarias, etc. **Y los usamos para diferentes cosas**: participar en actividades, mandarles comunicaciones, etc.
- **Algunos de los datos personales** que recogemos son datos, **según la ley**, más sensibles que otros y por tanto **los tenemos que proteger con mayor seguridad**, por ejemplo datos de salud, religión, raza, orientación sexual,...

2. ¿Qué leyes regulan la protección de datos?

a. **Constitución española de 1978.** ***(en vigor)***
Recoge como derecho fundamental la protección al honor y la intimidad personal y familiar de la ciudadanía. (Art. 18.1)

b. **Ley orgánica 15/99 de protección de datos de carácter personal (LOPD)** ***(aplicable desde 25 de mayo 2016 sólo en lo que no contradiga el Reglamento Europeo 2016/679)***
Establecía claramente las medidas para proteger los datos con obligaciones y derechos concretos: cómo informar, modificar, cancelar, etc. Recogía dos tipos de consentimiento de la persona afectada: tácito y expreso. Basada en un CUMPLIMIENTO PASIVO.

c. **Reglamento de desarrollo de la LOPD (Real decreto 1720/2007)** ***(aplicable desde 25 de mayo 2016 sólo en lo que no contradiga el Reglamento Europeo 2016/679)***

Detallaba todas las medidas de seguridad necesarias para proteger los datos y el procedimiento para ello.

d. **Reglamento 2016/679 General de Protección de Datos en la Unión Europea (RGPD)** ***(en vigor desde el 25 de mayo de 2016 y obligatorio a partir del 25 de mayo de 2018)***
Es de aplicación en todos los estados de la Unión Europea y para cualquiera que trate datos personales dentro de la Unión Europea y/o que se encuentre en la Unión Europea. Está por encima de las leyes nacionales de los estados miembros si éstas no están adaptadas a él.

Presenta cambios significativos respecto a la normativa anterior: el consentimiento tiene que ser expreso no tácito, las medidas de seguridad dependerán de cada organización en base a su evaluación de riesgos e impacto. Basado en una RESPONSABILIDAD PROACTIVA.

e. **Proyecto de Ley orgánica de Protección de datos (10/11/2017)** ***(pendiente de aprobarse)***
Establecerá las normas aplicables a la protección de datos adaptadas a lo que dice el RGPD de 2016. Consentimiento de menores estará en 13 años, mientras que en la actual es de 14.

3. ¿Cuáles son las ideas clave en la protección de datos?

- Consentimiento

El consentimiento tiene que cumplir dos condiciones: ser **inequívoco** (no puede ser tácito ni casillas pre-marcadas) y **para finalidades concretas** (si hay diferentes finalidades hay que dar consentimientos diferentes).

Para recabar el consentimiento previamente hay que informar a la persona porque el consentimiento tiene que ser un **consentimiento informado** (si se recoge la firma/ consentimiento de alguien que no ha sido bien informado es como si no se hubiera dado).

Hay **situaciones en las que no es necesario recoger el consentimiento: cuando hay una relación contractual, obligación legal, interés público, intereses vitales, o intereses legítimos** (p.ej. todas las asociaciones pueden usar los datos de sus personas asociadas para las actividades de la asociación sin necesidad de pedirles el consentimiento).

En el caso de menores de 14 años se tiene que recabar el consentimiento de su padre/madre o tutor/a.

- Responsable de tratamiento

  Es quien **decide sobre la finalidad, contenido y uso del tratamiento de los datos** aunque no lo realice materialmente. Por ejemplo nuestra asociación sería la responsable de todos los tratamientos de los datos de nuestras personas asociadas, lo hagamos desde la asociación o se lo encarguemos a alguien externo.

- Encargado/a de tratamiento

  Quien **trata datos personales por encargo de quien es responsable del tratamiento.** Por ejemplo si nuestra asociación encarga a una empresa de envíos postales que mande a las direcciones de todas las personas asociadas un ejemplar de la revista de la asociación, le tiene que facilitar esos datos y quien va a tratar esos datos es la empresa que hace el envío.

- Delegado/a de protección de datos

  Es una **figura nueva** que introduce el Reglamento Europeo y se establecen sus funciones, perfil profesional, posición en la entidad,... Se trata de una figura **fundamentalmente de supervisión**. Hay que especificar en la información que se da los datos de contacto de esta figura.

- Medidas de seguridad

  Son todas aquellas **acciones que se han de llevar a cabo para la protección correcta de los datos** siendo más exhaustivas en el caso de datos de especial protección (salud, religión, raza,...). Por ejemplo si vamos a tener las carpetas en papel con los datos de las personas voluntarias en un armario con llave y con acceso limitado, o si vamos a introducir algún sistema de contraseña o cifrado en los archivos que contienen datos dentro del ordenador de la asociación, etc.

4. ¿A qué estamos obligadas las asociaciones según las leyes de protección de datos?

Responsabilidad Proactiva = no sólo se trata de **cumplir con la ley** si no que **también** hay **que demostrarlo. Estamos obligadas a las siguientes acciones:**

- **Informar**

Tenemos la obligación de informar de qué datos queremos/tenemos, para qué los vamos a usar, durante cuánto tiempo, a quién se los vamos a ceder (en su caso), y dónde pueden acudir para modificarlos y cancelarlos (deben aparecer los datos de quien es Responsable del Tratamiento y de la persona Delegada de Protección de Datos). No vale consentimiento tácito ni casillas pre-marcadas.

Además **la información** que demos tiene que ser **concisa, transparente, inteligible y de fácil acceso, explicada con un lenguaje claro y sencillo.**

La **información se tiene que ofrecer por CAPAS o niveles**: Una primera información básica y resumida con la posibilidad de acceder a un segundo nivel de información más detallada. Por ejemplo en un formulario online se explica en una primera capa la finalidad para la que se van a usar los datos y se da un link a un documento en PDF en donde se detallan mucho más los fines del tratamiento, los plazos/criterios para conservar los datos, etc.

> *En este documento de la Agencia de protección de datos se dan orientaciones sobre cómo cumplir con el deber de informar: Guía modelo clausula informativa (pdf)*

- **Legitimación para tratar los datos:**

Las entidades **sólo podemos tratar los datos si estamos legitimadas para ello.** ¿Cómo podemos estar legitimadas? **Si se da alguna de las siguientes condiciones:**

- **Consentimiento informado** (cuando hemos recogido los datos con el consentimiento expreso e informado de la propia persona). *Ver punto 3.1 de este documento.*
- **Relación contractual** (cuando los datos se han dado por existencia de un contrato, verbal o escrito, y nos faculta para usar esos datos; por ejemplo cuando te contratan como empleado por cuenta ajena tienen que usar tus datos bancarios para que te paguen el salario, cuando pagas con una tarjeta de crédito realizas un contrato por el cual aceptas que puedan acceder a tus datos, etc.)
- **Intereses vitales de la persona interesada o de otras** (si alguien necesita asistencia sanitaria urgente se pueden usar sus datos aunque no haya dado su consentimiento)

- **Obligación legal para el responsable** (cuando hay una ley que obliga a que se recaben esos datos, por ejemplo cuando la empresa tiene que facilitar a la seguridad social los datos de sus empleados)
- **Interés público o ejercicio de poderes públicos** (por ejemplo cuando para la gestión de un servicio municipal: biblioteca, polideportivo, etc.; se tienen que usar los datos de los usuarios.)
- **Intereses legítimos del responsable o de un tercero** (por ejemplo el derecho a la libertad de información de los medios de comunicación puede prevalecer ante el derecho a la protección de datos en temas de corrupción política. Se tiene que valorar cuál de los intereses prevalece más.)

- Garantizar el ejercicio de los derechos del interesado/a

Las entidades **tenemos que garantizar que las personas interesadas puedan ejercer sus derechos** (aunque a veces se tienen que cumplir determinadas condiciones para ello) que son los siguientes:

- Derecho de **Información**: tienen derecho a estar informadas de qué datos, para qué finalidad, durante cuánto tiempo y quién los tiene.
- Derecho de **Acceso**: tienen derecho a solicitar el acceso a sus datos personales.
- Derecho de **Rectificación**: tienen derecho a modificar sus datos si están incompletos o son inexactos.
- Derecho a **Supresión** (derecho a **Olvido**): tienen derecho a solicitar que se supriman sus datos. En algunos casos no es posible suprimirlos totalmente (por ejemplo si hay una obligación legal de conservar los datos) pero sí se puede bloquear su acceso.
- Derecho a **Oposición**: tienen derecho a oponerse al tratamiento de sus datos. Por ejemplo decir que no quieren que su foto o sus datos salgan en la página web de la asociación.
- Derecho de **Limitación al tratamiento**: tienen derecho a solicitar la limitación de su tratamiento. Es decir que no quieren que se usen sus datos para determinadas cosas.
- Derecho de **Portabilidad**: tienen derecho a la portabilidad de sus datos. Por ejemplo cuando cambiamos de compañía telefónica tenemos derecho a llevarnos el número y que se le pase a otra compañía.

Imagen gráfica de los derechos de las personas interesadas:
Infografía derechos ciudadanos AEPD (pdf)

- Deber de confidencialidad

Las entidades estamos obligadas a la **confidencialidad de los datos** y es un deber que afecta a **cualquiera que trate los datos**: responsables,

encargados/as, voluntariado, personal remunerado,... incluso personas usuarias con respecto a otras usuarias.

- **Contrato entre responsable y encargado/a**

Es muy **importante que** cuando tratamos datos personales **sepamos cuál es nuestro papel**, si somos **responsables** del tratamiento de los datos (por tanto **decidimos para qué se usan) o** somos **encargadas** del tratamiento (no decidimos sino que **ejecutamos un encargo de quien decide**). Por ejemplo cuando cedemos los datos a una empresa para que nos hagan el envío de cartas somos las responsables y la empresa la encargada, pero cuando un ayuntamiento nos cede los datos de los niños apuntados a un campamento que nosotros vamos a gestionar seríamos las encargadas y el ayuntamiento el responsable.

La normativa obliga a que cuando se va a encargar a alguien el tratamiento de los datos se tiene que **firmar un contrato o convenio entre ambas partes** (responsable y encargada) donde se tienen que recoger los puntos estipulados en la normativa.

Además, es deber del **responsable elegir como encargada a quien le dé garantías suficientes de cumplimiento** de la normativa sobre protección de datos.

> *En este link se accede a una guía sobre directrices para los contratos entre responsables y encargados de tratamiento: Guía directrices contratos (pdf)*

- **Nuevas medidas de responsabilidad proactiva**

Son las **medidas que la nueva normativa obliga a adoptar** basadas en la filosofía de que además de cumplir con la protección de datos hay que demostrarlo. Las medidas que hay que seguir **son las siguientes**:

- **Registro de actividades de tratamiento:** ya no es necesario comunicar a la Agencia de Protección de Datos la existencia de ficheros en la entidad, sin embargo sí es obligatorio llevar un *registro de actividades interno actualizado*, en el que se indiquen los diferentes tratamientos de datos que realiza una entidad cuando se refiera a datos de especial protección (salud, religión, etc.).
- **Delegada o Delegado de Protección de datos:** es una figura obligatoria en todas las administraciones públicas y en muchas entidades y empresas privadas. Es la figura que garantiza el cumplimiento de la protección de datos en la entidad.
- **Gestión de la seguridad:** frente a unas medidas de seguridad basadas en función del tipo de datos personales, como exigía la normativa anterior, la nueva normativa establece que las medidas de seguridad a

adoptar serán aquéllas que se adecúen más a los riesgos detectados en la evaluación de los mismos. Se tendrá en cuenta también el estado de la técnica, los costes y los fines del tratamiento.

- **Privacidad desde el diseño y por defecto:** se trata de tener en cuenta siempre la privacidad para adoptar medidas organizativas y técnicas más adecuadas para proteger los datos personales. Por ejemplo valorar si no son estrictamente necesarios ciertos datos y no pedirlos.
- **Evaluaciones de impacto sobre la privacidad:** en algunas ocasiones será necesario hacer evaluaciones de impacto con carácter previo respecto a la privacidad para poner en marcha las medidas necesarias para evitar los posibles riesgos o minimizarlos.
- **Notificación de violaciones de seguridad:** Cuando se produce una brecha en la seguridad hay que notificarlo sin demora a la Agencia de Protección de datos (máximo 72 horas desde que se ha tenido constancia) y, en supuestos muy graves, también a las personas afectadas.
- **Códigos de conducta y certificaciones:** se promueve que existan códigos de conducta respecto a la protección de datos por parte de determinadas entidades o grupos de ellas en los que se exponen una serie de principios que se comprometen a cumplir. Igualmente se fomentan las certificaciones como medio de acreditar que se cumplen las obligaciones que conlleva la adhesión a un código de conducta.

5. ¿A dónde puedo acudir para solucionar dudas sobre la protección de datos?

La Agencia Española de Protección de Datos (https://www.aepd.es/) es la responsable para cualquier consulta que tenga que ver con personas físicas o entidades jurídicas privadas. Las agencias territoriales de Protección de Datos, como por ejemplo la **Agencia Vasca de Protección de Datos**, son las responsables de este tema para las entidades públicas de su territorio.

Por tanto, las asociaciones y entidades sin ánimo de lucro tendremos que dirigirnos para cualquier consulta a la Agencia Española de Protección de Datos.

También hay una web habilitada para ayudar en la protección de datos a menores: Protección datos menores

Desde el servicio de asesoramiento de **bolunta** (asesoria@bolunta.org) ofrecemos para las asociaciones orientaciones básicas sobre todo lo referente a este tema. También se oferta anualmente desde la oferta formativa de la agencia un curso sobre esta materia. Video tutorial OTS