INFORMACIÓN para IGLESIAS EVANGÉLICAS sobre Protección de Datos

ferede

INFORMACIÓN PARA LAS IGLESIAS EVANGÉLICAS SOBRE LAS OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS

I. NORMATIVA APLICABLE EN ESTA MATERIA

La normativa principal en materia de protección de datos personales la constituyen el Reglamento Europeo (UE) 2016/679, también conocido como RGPD, así como la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

Además de estas dos normas fundamentales, existen otras que inciden en el tratamiento de datos personales que puede realizar una iglesia, como es el caso de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, especialmente importante para aquellas iglesias que sean titulares de una página web.

II. ¿DE QUÉ MANERA RESULTA DE APLICACIÓN ESTA NORMATIVA A UNA IGLESIA O ENTIDAD RELIGIOSA?

Las iglesias y entidades religiosas, en la medida en que tengan y traten datos de carácter personal (datos personales de sus miembros, de sus donantes, de las personas de contacto, de los usuarios de la obra social, etc.), **están obligadas a adaptarse a las exigencias del Reglamento Europeo y de la Ley Orgánica.**

III. ¿CUÁLES SON LAS PRINCIPALES OBLIGACIONES PARA UNA IGLESIA EN ESTA MATERIA?

1. Cumplir con el Principio de Responsabilidad proactiva:

Al tratar datos de carácter personal, las Iglesias y entidades religiosas son responsables de ese tratamiento. Y según el este principio de responsabilidad proactiva, las entidades han de cumplir con responsabilidad y diligencia sus deberes como responsables de tratamiento, y tienen que poder acreditar el cumplimiento de cada exigencia derivada de cada tratamiento de datos de carácter personal.

Para ello es necesario que, en primer lugar, la entidad realice un examen exhaustivo de cada actividad de tratamiento que realice. Para ello, deberá hacerse las siguientes preguntas:

- ¿qué datos tenemos?
- ¿cómo los obtenemos?
- ¿para qué los recabamos?
- ¿a quién se los damos?
- ¿cómo los cuidamos?
- ¿cuándo y cómo los eliminamos?

Con esta información, la entidad tiene la obligación de proceder a un **análisis de los riesgos** que existen en la entidad con los datos de carácter personal con los que trabaje. Este análisis deberá quedar documentado y, con él, la entidad podrá detectar cuáles son los riesgos existentes en relación a los datos personales que trate. En consecuencia, deberá adoptar las medidas necesarias para evitar, prevenir y solucionar esos riesgos.

Si el riesgo es alto o se efectúan tratamientos a gran escala de datos especiales, se deberá hacer una **evaluación de impacto** que, igualmente, deberá quedar documentada.

Una vez que la entidad tenga claro los datos de carácter personal con los que trabaja y que trata, y que conozca los riesgos existentes a dichos datos, deberá adoptar las **medidas de carácter técnico y organizativo** que resulten apropiadas para garantizar que el tratamiento se lleve a cabo conforme al Reglamento, teniendo en cuenta, aparte de la naturaleza, ámbito, contexto y fines del tratamiento, los riesgos de diversa probabilidad y gravedad que el tratamiento puede tener para los derechos y libertades de las personas físicas.

La responsabilidad proactiva implica también hacer un examen de idoneidad de los proveedores de la entidad que, para prestarle servicios, deben tratar datos de los que la entidad es responsable (encargo del tratamiento); por ejemplo, los contratos con las gestorías o proveedores de servicios de páginas web.

2. Designar un Delegado de Protección de Datos:

Es necesario designar un Delegado de Protección de Datos cuando la actividad principal de la iglesia consista en el tratamiento a gran escala de categorías especiales de datos personales.

Si la Iglesia contrata el servicio de FEREDE, también podrá contar con la posibilidad de designar a esta Federación como su Delegado de Protección de Datos.

3. Prestar mucha atención a la hora de recabar el consentimiento.

Para tener y tratar datos de carácter personal, tiene que haber una base jurídica que autorice y motive tal tratamiento de datos, y hay que documentar tal base para poder demostrar su existencia. De lo contrario, la

entidad estaría cometiendo una infracción muy grave. Tal base jurídica, normalmente es la autorización y el consentimiento del titular de los datos de carácter personal.

El consentimiento:

- nunca podrá ser implícito, sino explícito y específico. Si alguna persona no quiere dar su consentimiento, sus datos de carácter personal no podrán ser recabados ni utilizados por la entidad.
- el consentimiento ha de ser otorgado en relación con cada tratamiento específico para el cual sea requerido, de forma individualizada. No se puede tener un consentimiento general que abarque diferentes finalidades sin que se especifiquen los tratamientos específicos y separados que se realizarán.
- el consentimiento tiene que ser informado, y esa información alcanza a la identidad del responsable del tratamiento y los fines a los cuales están destinados los datos personales, si va a haber transferencia de datos a países fuera de la UE, del derecho a revocarlo en todo momento y cualquier otra característica sustantiva.

4. Observar los principios de lealtad y transparencia.

El Reglamento exige que el interesado (el titular de los datos personales) tenga un conocimiento real sobre el tratamiento de los datos que se va a realizar. Esto implica que la entidad, al recabar el consentimiento, facilite suficiente información siguiendo las siguientes pautas que se entienden como "buenas prácticas":

- utilizar un lenguaje claro y sencillo, comprensible para todos,
- evitar remisiones a textos legales,
- situar las cláusulas informativas en lugares visualmente de fácil acceso.

5. Observar el principio de limitación de la finalidad:

Los datos se deben recoger con unos fines determinados, explícitos y legítimos, y si se van a utilizar posteriormente para otros fines, esos fines ulteriores deben ser compatibles con el fin original.

6. Observar el principio de minimización de datos:

La entidad debe recabar los datos que sean estrictamente necesarios, en relación con los principios de proporcionalidad y coherencia. No se deben recabar datos excesivos o no necesarios para conseguir la finalidad que se pretende.

A la hora de plantearse recoger y tratar posteriormente datos personales, se debería seguir el siguiente orden:

- determinar la finalidad para la que se van a recoger;
- determinar el tratamiento que se va a hacer;
- recabar los datos exclusivamente precisos.

7. Cumplir con el principio de exactitud:

Los datos deben ser correctos y actualizados. Por ello deben establecerse protocolos de actualización de los datos.

8. Cumplir con el principio de limitación del plazo de conservación:

Hay que identificar con claridad el plazo durante el cual se van a tratar o conservar los datos personales. Para ello, dotarse de un protocolo de supresión de los datos vinculado al registro de actividades de tratamiento para tener claro los plazos de conservación aplicables a cada tratamiento y un sistema para proceder a la supresión de los datos cuando efectivamente corresponda.

9. Conocer y proteger los derechos introducidos por la normativa:

Toda persona cuyos datos tratemos es titular de una serie de derechos en cuanto a su información: Derecho de Acceso, Rectificación, Supresión, Oposición, Limitación y Portabilidad del Tratamiento.
El derecho que con más frecuencia se ejerce respecto de una iglesia es el derecho de supresión de los datos personales y estas peticiones suelen llegar de parte de personas que dejan de formar parte de la iglesia o de tener relación con la misma.
Es necesario que a la hora de obtener el consentimiento se informe sobre la existencia sobre estos derechos, así como que se responda debidamente a las solicitudes de ejercicio.

10. Crear y mantener un Registro de Actividades de tratamiento

El Registro de actividades de tratamiento es un documento obligatorio para las Iglesias, al realizar tratamientos de datos personales que incluyen categorías especiales de datos personales, como son los datos relativos a la religión de las personas. El registro de actividades ha sustituido la anterior obligación de registro de ficheros en la Agencia Española de Protección de Datos.

Dicho registro debe incluir:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o a una organización internacional, y en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad adoptadas.

11. Régimen sancionador

El Reglamento Europeo ha incrementado aún más las sanciones económicas que pueden ser impuestas por cualquier incumplimiento, pudiendo llegar a imponer multas administrativas de hasta 20.000.000 de euros. A modo de ejemplo, si una iglesia recoge y tiene datos personales sin el necesario consentimiento del titular, sería constitutivo de una infracción muy grave que podría estar sancionada, según la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales con una multa superior a los 300.000 euros.

12. Obligación de dotarse de un protocolo o procedimiento de gestión de derechos:

Este protocolo ha de contener:

- canalización de solicitudes recibidas;
- persona encargada de dar respuesta;
- registro de las solicitudes recibidas;
- estudio de las solicitudes y respuesta;
- repositorio de formularios de solicitudes y respuestas;
- derivación de posibles incidencias y/o medidas correctoras. Ello para poder acreditar el cumplimiento de sus obligaciones.

IV. ¿QUÉ PASA CON EL TRATAMIENTO DE DATOS PERSONALES EN LOS ENTORNOS WEB Y REDES SOCIALES?

Desde que se aprobó la normativa de protección de datos actual, en 2016, hasta hoy, el uso de las redes sociales y los recursos online se ha visto multiplicado en todas las áreas, así ha sucedido igualmente en el ámbito de la iglesia, de modo que son muchas las entidades que disponen de página web y redes sociales como forma de darse a conocer e incluso de dar testimonio.

En el servicio jurídico con frecuencia recibimos consultas acerca de la posibilidad de subir imágenes y videos a la web y redes de la iglesia en la que aparezcan miembros o asistentes a las actividades.
Nuestra recomendación es que los equipos de multimedia y responsables de los recursos digitales de la iglesia se formen en esta materia, conozcan la normativa, y establezcan protocolos y medidas de seguridad para cumplir con la misma.

Las opciones para hacer un uso responsable pero efectivo de las redes sociales de la iglesia son diversas, y dependen de la situación concreta de cada iglesia, pero hay algunas obligaciones y principios básicos que cumplir como son el consentimiento, el principio de minimización y actualización de los datos.
El uso de la imagen personal en los entornos digitales y web es una de las áreas en las que más solicitudes de ejercicio de derechos y quejas puede recibir una iglesia, por lo que es conveniente que la misma sepa cómo responder a estas solicitudes y atenderlas debidamente.

V. ¿CÓMO PUEDEN CUMPLIR LAS IGLESIAS CON TODAS ESTAS EXIGENCIAS? FEREDE PUEDE AYUDAR A LA ENTIDAD.

Desde FEREDE consideramos que no es sencillo para una iglesia ni para sus responsables llevar a cabo, por sí mismos, este proceso de adaptación y cumplimiento normativo, salvo que cuenten entre sus miembros o contactos con algún especialista en la materia.

Por ello, consideramos que es importante un apoyo externo, y por eso **FEREDE ha preparado un servicio específico en materia de Protección de Datos para iglesias y entidades evangélicas.**

Esta iniciativa responde a la petición de muchas entidades que así lo han demandado, y a nuestro convencimiento de que, al llevar más de sesenta años ayudando a las entidades evangélicas, conocemos perfectamente su funcionamiento y podemos prestarles un servicio adaptado a sus necesidades.

Si vuestra entidad está interesada en recibir esta ayuda y acceder a este servicio, no tiene más que escribir a protecciondatos@ferede.org, o llamar al 913810402, donde les informaremos de todos los detalles.