

INFORME SOBRE LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LAS IGLESIAS Y ENTIDADES RELIGIOSAS EVANGÉLICAS

- I. Normativa aplicable
- II. ¿Cuál es la finalidad de la normativa de protección de datos?
- III. Pronunciamiento del Tribunal Supremo con respecto a la aplicación de la legislación de protección de datos a la Iglesia Católica.
- IV. Aplicación la normativa sobre protección de datos a las Iglesias y demás entidades Evangélicas
- V. Obligaciones de las Iglesias en materia de protección de datos.
- VI. Anexos

I. NORMATIVA APLICABLE

La legislación de protección de datos encuentra su fundamento en el artículo 18 de la Constitución española, que garantiza el derecho al honor y a la intimidad personal y familiar de los ciudadanos.

Para garantizar este derecho, y para adaptar nuestro ordenamiento jurídico a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, se aprobó la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal.

En desarrollo de esta Ley, se aprobaron diferentes reglamentos, entre ellos:

- El Real Decreto 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la Agencia de Protección de Datos.
- El Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 26 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal
- El Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Con posterioridad, fue aprobado el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 anteriormente mencionada. Este reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994 y el 994/1999, y además desarrolla los procedimientos para el ejercicio de la potestad sancionadora de la Agencia de Protección de Datos.

Lo que se pretende con este informe es explicar y realizar un resumen no exhaustivo de lo que es de aplicación a las iglesias y entidades evangélicas en materia de protección de datos. Es por ello que facilitamos la normativa aplicable, para que cada iglesia pueda con posterioridad profundizar en este tema cuando se disponga a implantar todas las medidas de seguridad que correspondan.

II. ¿CUÁL ES LA FINALIDAD DE LA NORMATIVA DE PROTECCIÓN DE DATOS?

Toda esta normativa tiene por **objeto proteger el tratamiento de los datos de carácter personal de las personas físicas**, y se aplicará tanto a las entidades jurídicas o particulares que se encuentren en territorio español y tengan ficheros físicos con datos de carácter personal.

Un dato de carácter personal es cualquier información concerniente a personas físicas identificadas o identificables, y comprende, por ejemplo, datos tales como el nombre, apellidos, datos de identificación (DNI, NIE o pasaporte), imágenes que permitan la identificación de personas, etc. A estos datos, siempre que los incorporemos a un fichero que pueda ser objeto de tratamiento (tanto en papel como en manera automatizada), les resultarán aplicables los contenidos de toda esta normativa.

Quedan excluidos, sin embargo, los siguientes datos:

- Los datos referidos a las personas jurídicas, o los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales (por ejemplo, un listado de empresas, que recoge los datos personales de su director o administrador, con sus datos básicos de contacto, o por ejemplo, un listado de iglesias, que incluyen los datos de una persona de contacto).
- Los datos relativos a empresarios individuales cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.
- Los datos de personas fallecidas.

Esta normativa tampoco será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, que se inscriban en el ámbito de la vida privada o familiar.

III. PRONUNCIAMIENTO DEL TRIBUNAL SUPREMO CON RESPECTO A LA APLICACIÓN DE LA LEGISLACIÓN DE PROTECCIÓN DE DATOS A LA IGLESIA CATÓLICA

En algunos medios se ha llegado a decir que la Iglesia católica no está sometida o no se le aplica esta legislación. Como este asunto ha generado cierta confusión nos parece importante abordar el tema porque como luego se verá, también pueden derivarse conclusiones para nuestras Iglesias.

Lo primero que tenemos que decir es que la Iglesia Católica está afectada por la normativa de Protección de Datos, pues no se encuentra excluida de su ámbito de aplicación, en tanto y cuando maneje datos de carácter personal de los incluidos en esta normativa. De hecho, se pueden constatar que en la propia Agencia de Protección de Datos existen numerosos ficheros inscritos por parte de Parroquias y otro tipo de entidades católicas. A modo de ejemplo, constan ficheros de párrocos, sacerdotes y personal de contacto, ficheros de los miembros de los distintos grupos adscritos a las parroquias, ficheros del personal contratado, ficheros con datos de curriculum, ficheros de alumnos en entidades católicas educativas, etc.

Lo que ha originado cierta discusión es sobre la aplicación de la normativa a en algunos supuestos. Concretamente el **Tribunal Supremo** ha tenido oportunidad de pronunciarse respecto a los datos de carácter personal que constan en los libros parroquiales de las parroquias católicas, esto es, en libros de bautismos, libros de confirmación, matrimonio y defunción.

El caso se origina con la negativa de la Iglesia católica a la solicitud que una persona que queriendo ejercer la apostasía de esta confesión, pidió además la cancelación de los datos de su bautismo en el Libro de Bautismos de su parroquia. La Audiencia Nacional no accedió a esta petición, pero sí impuso al Arzobispado de Valencia la obligación de anotar por nota marginal en el Libro de Bautismo la solicitud de cancelación de aquella inscripción, al amparo de la LO 15/99. En esta sentencia la Audiencia entendió que los libros de bautismos son ficheros que contenían datos de carácter personal, en contra incluso del criterio de la entonces Dirección General de Asuntos Religiosos, que afirmaba que la Iglesia Católica no poseía ficheros de datos de carácter personal. Esta sentencia fue recurrida ante el Tribunal Supremo, que en fecha de 19 de septiembre de 2008 anuló la sentencia de la Audiencia Nacional en base a los siguientes argumentos:

- En primer lugar, porque los libros de bautismo no constituyen “ficheros” a efectos de la legislación sobre protección de datos, ya que los datos personales recogidos en los libros de bautismo no son un conjunto organizado, tal y como exige el artículo 3.b de la Ley Orgánica 15/99, sino que resultan una pura acumulación de éstos que comporta una difícil búsqueda, acceso e identificación, en cuanto no están ordenados, ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo, siendo absolutamente necesario el conocimiento previo de la parroquia donde aquél tuvo lugar, no resultando además accesibles para terceros distintos del bautizado, que no podrían solicitar ajenas partidas de bautismo. Y es que los ficheros no se conciben como un mero depósito de datos, que es en realidad lo que ocurre con los que se recogen en los libros de bautismo, cuyos datos son facilitados de manera voluntaria.
- En los datos reflejados en los libros de bautismo no cabe apreciar ninguna inexactitud, puesto que recogen datos históricos (salvo que se acredite su falsedad), cual es el referente al bautismo de una persona. Si alguien solicita la cancelación de este hecho, no está pretendiendo que se corrija una inexactitud en cuanto al dato concreto, sino que está intentando y solicitando un sistema nuevo y diferente de registro de nuevos datos personales.
- La Directiva 46/1995 del Parlamento Europeo, al regular la protección de datos y la regulación de su tratamiento, en su 15 considerando establece que "los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando estén automatizados, o cuando los datos a que se refieren se encuentren contenidos, o se destinen a encontrarse contenidos, en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trate". Sólo abarca por lo tanto a los ficheros, y no a las carpetas que no están estructuradas. Los libros de bautismo no tienen naturalmente la definición de recopilación de datos automatizados, sino manual, y esos datos no tienen que ver con la

permanencia o abandono de la religión católica, pues los libros de bautismo no constituyen una relación de miembros de dicha religión ni acreditan la permanencia en la misma de quienes fueron bautizados.

- Existen muchas dificultades para obtener información sobre el bautismo; en primer lugar la solicitud solo puede realizarse por el propio afectado.
- La utilización de los datos de los libros de bautismo para fines históricos, estadísticos o científicos no vulnera la Ley de Protección de Datos.

El Tribunal Supremo en sus pronunciamientos no está valorando si las entidades religiosas están o no sometidas a la normativa de protección de datos, pues lo están claramente. Lo que analiza es si determinados libros de la iglesia católica que contienen datos personales quedan dentro del ámbito de aplicación de esta normativa, concluyendo concretamente que los libros de bautismo de cada parroquia no pueden considerarse como ficheros propiamente dichos, y por ello no se puede ejercer contra los datos que contiene el derecho de cancelación.

IV. APLICACIÓN DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS A LAS IGLESIAS Y DEMÁS ENTIDADES EVANGÉLICAS

Por lo expuesto anteriormente, si una Iglesia o entidad evangélica maneja ficheros con datos de carácter personal, a los mismos les resultará de aplicación todo lo referido a su protección contenido en la Ley Orgánica 15/1999 de Protección de Datos y su reglamento de desarrollo.

En la práctica, las Iglesias evangélicas y otras entidades religiosas suelen tener los siguientes ficheros con datos de carácter personal en su funcionamiento cotidiano:

- Ficheros con los datos de los miembros, o libros de miembros.
- Los libros parroquiales, tales como libros de bautismos, de matrimonios y de defunciones, al igual que la Iglesia Católica.
- Ficheros de contactos.
- Ficheros de personal contratado.
- Ficheros de las personas atendidas o usuarios de las obras sociales, por ejemplo.
- Cualquier otro fichero con datos de carácter personal que sirva a sus fines específicos.

Con respecto a los libros de bautismos, matrimonios y defunciones, los mismos argumentos utilizados por el Tribunal Supremo para la Iglesia Católica podrían ser aplicados a las iglesias evangélicas, en el sentido de que se trata de datos de carácter histórico, que recogen acontecimientos que forman parte de la historia de la iglesia y sobre los que no cabe inexactitud (salvo que pueda existir algún error). Si además estos libros no estuvieran informatizados, nos encontraríamos en la misma situación que la Iglesia Católica, y se podría argumentar por ello que son libros que estarían fuera del ámbito de aplicación de la legislación de protección de datos.

Con respecto a los libros de membresía, que normalmente están informatizados, encajan perfectamente en la consideración de “fichero” con datos de carácter personal objeto de

tratamiento, tales como nombre, apellido, fecha de nacimiento, sexo, etc. De hecho, el artículo 7.2 de la Ley Orgánica de Protección de Datos expresamente habla de los ficheros de las iglesias, confesiones o comunidades religiosas que recojan datos relativos a sus asociados o miembros, estableciendo que con respecto a los mismos no será necesario el consentimiento expreso y por escrito para el tratamiento de los datos de carácter personal de los mismos, puesto que la solicitud de membresía ya incluye implícito este consentimiento.

Lo mismo sucedería en el caso de otro tipo de registros, tales como los ficheros con datos de contactos de la iglesia, que se suelen tener para enviar información sobre las actividades de la misma, o ficheros con datos de usuarios de determinadas actividades que se desarrollen (campamentos, reparto de alimentos, etc.)

Por lo tanto, las iglesias y demás entidades religiosas evangélicas tendrán que identificar cuáles son los distintos ficheros con datos de carácter personal que tienen, y adoptar con respecto a los mismos las medidas de seguridad que correspondan según la normativa de protección de datos.

¿Con qué tipo de datos suelen trabajar las entidades evangélicas?

La Ley de Protección de Datos distingue tres tipos de datos, los datos que requieren un nivel de protección básico, los que requieren un nivel de protección medio, y un nivel de protección alto. Las medidas de seguridad que es necesario adoptar varían en función de cada nivel de protección.

Los datos especialmente protegidos son aquéllos que hagan referencia a la ideología, religión o creencias, y los datos que hagan referencia al origen racial, a la salud y a la vida sexual.

Es probable, por tanto, que muchos de los datos que tienen las entidades evangélicas puedan estar especialmente protegidos, pues están referidos de manera directa a su religión y creencias. El libro de miembros de una iglesia, por ejemplo, recoge datos de carácter personal que se refieren directamente a la religión que profesan esas personas, por lo que estaríamos ante datos sensibles que tienen el máximo nivel de protección.

V. OBLIGACIONES DE LAS IGLESIAS EN MATERIA DE PROTECCIÓN DE DATOS

Para saber cuáles son las obligaciones existentes en materia de protección de datos es recomendable la lectura de la normativa aplicable y enumerada en el apartado primero de este documento.

En primer lugar, la iglesia o entidad tendría que examinar con cuántos ficheros de datos de carácter personal está trabajando. Éstos serán los ficheros con respecto a los cuales tendrá que adoptar las medidas de seguridad que en apartados posteriores se señalarán.

Las obligaciones que tienen las Iglesias que tengan ficheros de carácter personal podrían agruparse en 4 apartados. Estas cuatro fases están íntimamente relacionadas y tendrán que realizarse de manera simultánea:

- 1.- Notificar la creación del fichero o los ficheros que contengan datos personales a la Agencia Española de Protección de Datos.
- 2.- Elaborar un documento de seguridad en el que se detallen los criterios y medidas y procedimientos que la Iglesia debe y tienen acordado adoptar para garantizar el cumplimiento de los derechos y obligaciones de la Ley.
- 3.- Designar un responsable de seguridad.
- 4.- Aplicar y auditar las medidas contenidas en el documento de seguridad.

A continuación detallamos un poco la información sobre estos apartados:

1.- Notificar la creación del fichero o los ficheros que contengan datos personales a la Agencia Española de Protección de Datos.

Según lo establecido en la Ley de Protección de Datos, antes de crear un fichero de datos de carácter personal habrá que proceder a notificar la creación de los mismos a la Agencia Española de Protección de Datos (de hecho, la ausencia de dicha notificación sería constitutivo de una infracción leve según el artículo 44 de dicha ley). Si una iglesia ya cuenta con ficheros de datos de carácter personal, después de haber identificado cuáles son, tendrá que proceder, lo antes posible, a notificar su existencia ante la Agencia que corresponda (estatal o autonómica).

Esto no implica que la Iglesia o entidad tenga que facilitar los datos de las personas que tenga en sus ficheros, sino que simplemente comunicará la existencia del fichero y del tipo de datos que se recogen en el mismo. Por ejemplo, uno de los ficheros que toda iglesia tendrá que comunicar, será el fichero de miembros, indicando que en el mismo se recogen el nombre, los apellidos, la fecha de nacimiento, la dirección del mismo, etc.

El procedimiento para inscribir los ficheros es sencillo, y consiste en rellenar un formulario que podremos encontrar en la página web de la Agencia Española de Protección de Datos (https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/index-ides-idphp.php). Una vez completado y debidamente firmado por el responsable de los ficheros, este formulario se podrá presentar de manera telemática o en formato papel, enviándolo a la dirección de la propia Agencia.

Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Es importante recordar que no sólo hay que notificar a la Agencia la creación de los ficheros, sino que también habrá que inscribir la supresión o modificación de los mismos.

2.- Elaborar un documento de seguridad.

Todas las medidas de seguridad que es necesario adoptar se encuentran reguladas en los artículos 79 a 104 del Reglamento, y deberán constar explicadas en el documento de seguridad correspondiente de la entidad, que es obligatorio crear y mantener. Es muy importante que el responsable o responsables de seguridad manejen y conozcan el contenido del Reglamento, y es por ello que se facilita el mismo en la página web de FEREDe junto a este informe. En el documento se deben detallar los criterios, medidas y procedimientos que la Iglesia que debe y tiene acordado adoptar para garantizar el cumplimiento de los derechos y obligaciones contenidos en la normativa.

Este documento no ha de remitirse a la Agencia Española de Protección de Datos, sino que la entidad tiene que disponer del mismo y aplicarlo para evitar posibles sanciones. En la propia página web de la Agencia se facilita un modelo de documento de seguridad que puede utilizarse como guía para elaborar el propio documento de seguridad de la Iglesia o entidad evangélica (https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf).

El documento de seguridad deberá contener información al menos sobre los siguientes asuntos:

- a) Identificación de la entidad y del ámbito objetivo del Documento de Seguridad,
- b) Designar un Responsable de Seguridad
- c) Explicar cómo se gestionan los soportes y documentos donde se almacena la información
- d) Establecer procedimientos de ejecución y seguridad para las copias de respaldo y recuperación de la información.
- e) Definir y documentar las funciones y obligaciones del personal
- f) Identificar y autenticar a los usuarios
- g) Disponer de controles y registros de accesos a la información
- h) Explicar la forma de gestión de los accesos a través de las redes de comunicaciones
- i) Prever y gestionar las incidencias de seguridad
- j) Efectuar Auditorías y Controles periódicos

3.- Designar un responsable de seguridad

El encargado de aplicar en la Iglesia la normativa de protección de datos según consta en el documento de seguridad es el responsable o responsables de seguridad.

Para implantar y cumplir la normativa de protección de datos, deberá existir en la entidad una o más personas que sean designadas como responsable de seguridad, que deberá formarse en esta materia, y que se tendrá que responsabilizar del cumplimiento de todas las medidas de seguridad que consten en el correspondiente documento de seguridad del que ya hemos hablado.

La obligación del responsable de seguridad es velar por el cumplimiento en una determinada entidad de las normas de seguridad (enumeradas anteriormente) contenidas en el Documento de Seguridad y en la normativa de protección de datos.

En concreto sus funciones y obligaciones son:

- Determinar y describir los recursos informáticos a los que se aplicará el Documento de Seguridad.
- Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
- Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos y su periodicidad.
- Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al Sistema Informático, con especificación del nivel de acceso que tiene cada usuario.
- Establecer y comprobar la aplicación del procedimiento de identificación y autenticación de usuarios, así como la asignación, distribución y almacenamiento de las contraseñas de acceso.
- Establecer y comprobar la aplicación del procedimiento de cambio periódico de las contraseñas de los usuarios del sistema.
- Establecer y comprobar la aplicación de un sistema que limite el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Establecer y comprobar la aplicación de los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.
- Conceder, alterar, anular el acceso autorizado a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.
- Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas.
- Establecer los controles periódicos y auditorías necesarias para comprobar el nivel de cumplimiento del documento.

En resumen, el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos. Y además de implantar las medidas, tendrá que efectuar una auditoría cada dos años para verificar el estado de cumplimiento de las normas en materia de protección de datos, elaborando informes que dejen constancia de los controles efectuados y de las medidas correctoras adoptadas.

Es importante destacar que se producirse una inspección de la Agencia de Protección de Datos, y de imponerse una sanción, ésta sería impuesta en principio a la entidad responsable de los ficheros, no se impondría al responsable de seguridad.

4.- Aplicar y auditar las medidas contenidas en el documento de seguridad

4.1.- ¿Cómo implementar todas estas medidas en la Iglesia?

Las entidades religiosas tienen dos opciones: que alguno de sus miembros se forme en esta materia y se encargue de implementar todas las medidas de seguridad necesarias, o bien que se contraten los servicios de algún profesional o empresa que se dedique expresamente a la implantación de tales medidas. En este último caso, no obstante, será también necesario que alguna persona de la iglesia se forme y se prepare, pues deberá encargarse del seguimiento y la aplicación cotidiana de todas las medidas de seguridad que se implanten.

Desde FEREDE se ha trabajado para ofrecer el presente documento junto con los textos legales necesarios para que las iglesias puedan tener un primer acercamiento a esta materia. A través de la página web se publicarán las novedades y modificaciones que puedan surgir en torno a esta normativa de obligado cumplimiento.

No obstante, cualquier pregunta o consulta podrá realizarse en las oficinas de esta Federación, bien sea a través del teléfono o del correo electrónico (juridico@ferede.org). Trataremos de resolver las dudas que puedan surgir en torno a la aplicación de toda esta normativa.

Además, hemos de citar que algunos profesionales evangélicos, conocedores de la realidad interna de nuestras iglesias y que se dedican profesionalmente a la protección de datos, se han puesto en contacto con FEREDE para ofrecer sus servicios a las iglesias evangélicas que deseen contratarlos. Es por ello que desde esta Federación se facilitarán los datos de contacto de los mismos por si alguna entidad estuviera interesada.

4.2.- ¿Cómo aplicar estas medidas en la relaciones de la Iglesia con las personas?

Las medidas de seguridad que hay que adoptar con respecto a la protección de datos son variadas, y se encuentran recogidas en el Reglamento. No obstante, una vez inscritos los ficheros, creado el documento de seguridad, nombrado el responsable de seguridad y adoptadas todas las medidas de seguridad, la Iglesia ha de saber que con todos los datos de carácter personal con los que trabaje tendrá siempre que **recabar el consentimiento del afectado**, y **garantizar al mismo el ejercicio de los derechos que le reconoce la ley** (llamados derechos ARCO). A continuación facilitamos información algo más detallada sobre estas dos cuestiones que la iglesia siempre tendrá que tener en consideración:

I.- Recabar el consentimiento del afectado

Para poder recabar y tratar datos de carácter personal es imprescindible la obtención del consentimiento del afectado, excepto en aquellos casos en los que la obtención del consentimiento no sea exigible con arreglo a lo dispuesto en las leyes.

Para obtener el consentimiento es necesario que el responsable del fichero informe al interesado de la finalidad para la que recaba los datos y si sus datos van a ser cedidos y con qué fines. En caso de problemas, es el responsable del fichero (el que recaba los datos) el que tiene que probar que existió el consentimiento. Es por ello que siempre es recomendable obtener el consentimiento de manera expresa y por escrito.

Se prevé también la posibilidad del consentimiento tácito, que se recabaría dirigiéndose al afectado y concediéndole un plazo de 30 días para manifestar su negativa al tratamiento de sus datos, facilitando un medio sencillo y gratuito para manifestar su negativa al tratamiento de sus datos. No obstante, no es posible obtener el consentimiento tácito en los datos que están especialmente protegidos. En estos casos es imprescindible el consentimiento expreso y escrito.

Ya hemos hecho referencia a que el artículo 7.2 de la Ley Orgánica establece que en el caso de los datos relativos a los miembros de las iglesias, no es necesario recabar el consentimiento expreso y por escrito para el tratamiento de sus datos de carácter personal, puesto que la solicitud de membresía ya incluye implícito este consentimiento. Es recomendable, no obstante, incluir en las solicitudes de membresía de las iglesias (al igual que en todos los documentos mediante los cuales se recaben datos de carácter personal), la siguiente cláusula informativa:

“De conformidad con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, consiento que mis datos sean incorporados a un fichero responsabilidad de la Iglesia (nombre de la entidad que corresponda) y que sean tratados con la finalidad de *mantener y desarrollar mi pertenencia como miembro en la misma*¹.

Asimismo declaro haber sido informado sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndome a la Iglesia, sita en la calle, nº , piso....., CP, población; o bien remitiendo un mensaje a la dirección de correo electrónico²”

El consentimiento que se recabe ha de ser un consentimiento informado; el responsable del fichero que solicite datos de carácter personal tendrá informar previamente (y tendrá además que probar si informó de todo ello) al interesado de modo expreso, preciso e inequívoco de lo siguiente:

- De la existencia de un fichero o tratamiento de datos de carácter personal.
- De la finalidad de la recogida de los datos y de los destinatarios de la información
- Del carácter obligatorio o facultativo de las respuesta que le sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición
- De la identidad y dirección del responsable del fichero.

Lógicamente el consentimiento puede ser revocado en cualquier momento, y en ese caso no podrán tenerse ni tratarse los datos personales de esa persona en concreto.

Este tipo de cláusulas deberán ser utilizadas siempre por la Iglesia para recabar el consentimiento expreso de toda persona que de sus datos a la entidad. Por ejemplo, los beneficiarios de la obra social de la entidad (si es que se recogen sus datos personales y se incorporan a un fichero), a los contactos o asistentes de la iglesia, a las personas que participen en alguna actividad de la entidad (campamentos, etc.)

Se anexan a este documento otras cláusulas informativas que la entidad que afronte la adopción de todas estas medidas puede utilizar en sus recogidas de datos de carácter personal, en su correspondencia, en su correo electrónico, en su web, etc.

1 La finalidad descrita es orientativa; cada entidad tendrá que adaptar esta redacción, ajustándola a la finalidad para la que se recaben los datos de carácter personal.

2 Hay que establecer un mecanismo sencillo y gratuito para que los interesados puedan ejercitar sus derechos ARCO.

II.- Garantizar el ejercicio de los derechos ARCO

Cualquier persona, cuyos datos personales figuren en un fichero, cuenta con un conjunto de derechos a su alcance. En este sentido, todo Responsable de Ficheros con datos de carácter personal tendrá unas obligaciones para garantizar a los afectados el ejercicio de estos derechos. La Iglesia ha de conocer estos derechos y facilitar su ejercicio en todo momento. Son los siguientes:

- A. Acceso.
- B. Rectificación.
- C. Cancelación.
- D. Oposición.

A fin de garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, el Reglamento dispone que deberá concederse al afectado o interesado un medio sencillo y gratuito que en ningún caso podrá suponer un ingreso adicional para el responsable del fichero o tratamiento ante el cual tales derechos se ejercitan. Por dicha razón, el Reglamento declara expresamente contrarios a la normativa los supuestos en los cuales el responsable del fichero o tratamiento establece como medio para que el afectado o interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes.

Como novedad, se regula expresamente el derecho de oposición, en términos parecidos a la forma de revocar el consentimiento antes indicada, y se introduce la obligación al encargado del tratamiento de satisfacer los mencionados derechos si así se prevé en el contrato suscrito al efecto con el responsable. Asimismo, en línea con lo previsto respecto del cumplimiento de los deberes de informar y recabar el consentimiento, corresponde al responsable la prueba de haber dado respuesta, en el plazo previsto para cada uno de ellos, a la petición de los interesados, debiendo conservar acreditación de su cumplimiento.

Es muy importante que la Iglesia, como responsable del fichero, responda ante la petición del interesado, porque en caso contrario éste podría interponer una reclamación ante la Agencia Española de Protección de Datos.

A. Derecho de acceso

Permite al afectado preguntar al responsable del fichero si tiene datos personales suyos, cuáles, el origen de los mismos y la fuente. El derecho de acceso permite al afectado obtener información sobre si sus datos personales son objeto de tratamiento, la finalidad del tratamiento, si han sido objeto de cesión y la procedencia de los datos.

Para ejercitar el derecho de acceso, el afectado debe enviar una comunicación al responsable del fichero que deberá de cumplir con los siguientes requisitos:

- Nombre y apellidos. Acreditando claramente su identidad mediante copia de su D.N.I., pasaporte o documento equivalente. En el caso que el derecho de acceso se ejercite a través

de medios electrónicos, la utilización de la firma electrónica identificativa del afectado exime la presentación de la copia del D.N.I. o documento equivalente.

- Solicitud concreta.
- Dirección del afectado a efectos de notificaciones.
- Fecha de la solicitud.
- Firma del solicitante.
- Documentos acreditativos, en su caso.

El afectado puede optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia (Fax).
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema que sea adecuado a la configuración material del fichero o a la naturaleza del tratamiento.

El responsable del fichero debe resolver sobre la solicitud de acceso en el plazo máximo de 1 mes desde la recepción de la petición. Si resuelve no permitir el ejercicio del derecho de acceso, también deberá notificarlo al afectado.

B. y C. Derechos de rectificación y cancelación

Es el derecho que tiene el afectado a que se modifiquen los datos que resulten ser inexactos o incompletos, y que da lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo que el responsable del fichero puede tener.

Para ejercitar los derechos de rectificación y cancelación, el afectado debe dirigirse al responsable del tratamiento solicitando la rectificación o cancelación de sus datos.

Sendos derechos deben hacerse efectivos por parte del responsable del fichero en el plazo de 10 días hábiles siguientes a la recepción de la solicitud. En el caso en que los datos rectificadas o cancelados hubieran sido cedidos previamente a otra persona física o jurídica, el Responsable del Fichero notificará al cesionario la rectificación o cancelación para que éste la lleve a cabo en su fichero y en idéntico plazo

Cuando exista una disposición legal que exija la conservación de los datos personales sobre los que el afectado quiere ejercitar su derecho de rectificación o cancelación, no procederá el ejercicio de dichos derechos. En todo caso, quedarán bloqueados tanto para poder dar cumplimiento a obligaciones legales así como para poder ejercitar el derecho de defensa en su caso.

D. Derecho de oposición

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese de dichos tratamientos

- En aquellos casos en los que no sea necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal cuando existan motivos fundados y legítimos a una concreta situación personal, siempre que una Ley no disponga lo contrario.

- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado basada únicamente en un tratamiento automatizado de sus datos.

Para ejercer el derecho de oposición ser necesario:

- Solicitud dirigida al responsable del fichero.
- Cuando el tratamiento no requiere el consentimiento del afectado, será necesario exponer los motivos legítimos relativos a su situación personal que justifiquen tal hecho

El Responsable del Fichero resolverá sobre la solicitud de oposición en el plazo máximo de 10 días a contar desde la fecha de recepción. Si el responsable del fichero no dispone de datos personales del afectado, deberá comunicárselo

4.3.- ¿Qué consecuencias puede tener no cumplir con la normativa de Protección de Datos?

La normativa de protección de datos prevé un régimen sancionador muy severo, con sanciones consistentes en multas que pueden oscilar de entre los 600 hasta los 300.000 euros. Además, algunos de los datos que manejan las entidades religiosas son especialmente sensibles, por lo que las sanciones que pudieran ser de aplicación serían las más elevadas.

Es importante tener en cuenta que constituye infracción grave mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad expuestas.

MODELOS ANEXOS

CIRCULAR INFORMATIVA SOBRE LA ADOPCIÓN DE LAS NORMAS DE PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

La presente comunicación debe remitirse a todas aquellas personas físicas –que no sean empresarios individuales ni personas de contacto de una Organización- de las que se tengan datos de carácter personal, a fin de dar cumplimiento al deber de información regulado por el artículo 5 de la LOPD. Esta comunicación deberá llevarse a cabo en el momento de adaptarse a la LOPD.

En, a de de 201..

Muy Sr./a nuestro/a,

La presente circular tiene por objeto poner en su conocimiento que, en cumplimiento de lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en lo sucesivo, RDLOPD), la Iglesia(nombre de la entidad) ha implementado las medidas de seguridad técnicas y organizativas que son de obligado cumplimiento para todas las organizaciones, tanto públicas como privadas.

Es nuestro deber informarle que como consecuencia de la relación que nos une sus datos han sido incorporados a un fichero debidamente inscrito en el Registro General de Protección de Datos a nombre de esta entidad. La finalidad del tratamiento de estos datos es la de mantener, desarrollar y controlar la relación de membresía que le une a esta entidad.³

La Iglesia se compromete a cumplir con lo dispuesto por la normativa anteriormente mencionada, así como a hacer cumplir las medidas de seguridad técnicas y organizativas implementadas al personal a su servicio que trate datos de carácter personal. Dicho personal se halla sujeto al deber de secreto y confidencialidad en los mismos términos que la presente entidad.

Por otro lado, le informamos que de conformidad con lo dispuesto por el artículo 5 de la LOPD, podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición en la siguiente dirección: Calle, número ..., piso, CP, población.....; o bien remitiendo un mensaje de correo electrónico a la siguiente dirección

Sin otro particular, le saluda atentamente,

D./Dña.
Representante Legal

³ La finalidad descrita es orientativa; cada iglesia deberá adaptarla en orden a reflejar los tratamientos de los datos personales realmente realizados o previstos.

CIRCULAR INFORMATIVA PARA COLGAR EN EL LOCAL DE LA IGLESIA O ENTIDAD

La presente circular deberá situarse en un lugar visible de las instalaciones de la Iglesia o entidad religiosa (recepción, tablón de anuncios, oficinas administrativas...), en caso de que se recaben datos de carácter personal de forma verbal. No es frecuente, pero lo adjuntamos como modelo para que pueda ser utilizada.

En, a ... de ... de 2011

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, LOPD), se informa de los siguientes aspectos:

- La Iglesia es a los efectos de la LOPD, Responsable del Fichero, en el que se incluirán los datos personales que usted nos facilite. Dicho fichero consta debidamente inscrito en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.
- La finalidad del tratamiento de los datos será la que se defina para cada caso concreto, cumpliendo siempre con el debido respeto a los principios de calidad y proporcionalidad, definidos en el artículo 4 de la LOPD; es decir, los datos obtenidos serán siempre adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para la que fueron recabados.
- Podrá usted ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndose a la Iglesia, en calle, número, piso, CP, población; o bien remitiendo un mensaje a la dirección de correo electrónico"

CLAÚSULA INFORMATIVA PARA LA WEB

Es recomendable que la presente cláusula se incluya en aquellas páginas web en las que se recaben datos de los interesados –p.ej. mediante formularios o cuestionarios–, o bien se permita a los mismos contactar con la iglesia o entidad a través de correo electrónico.

“De conformidad con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, consiento la inclusión de mis datos en un fichero del que es titular la Iglesia, y que los mismos sean utilizados para **indicar finalidad del tratamiento de los datos**⁴. Asimismo, declaro estar informado sobre los derechos de acceso, rectificación, cancelación y oposición que podré ejercitar en el domicilio de esta entidad, en la calle, nº, CP, de; o bien remitiendo un mensaje a la dirección de correo electrónico indicando en el asunto “Protección de Datos”.

Para continuar debe usted aceptar que ha leído y está conforme con la cláusula anterior.

ACEPTO

⁴ Debe indicarse la finalidad del tratamiento o tratamientos que se prevean realizar la iglesia o entidad (p.ej. “envío de información sobre las actividades de esta entidad, etc.”

CLAÚSULA INFORMATIVA DEL CORREO ELECTRÓNICO

Esta cláusula deberá ser introducida como predeterminada en las firmas de correo electrónico, en aras a cumplir con el deber informativo recogido en el artículo 5.1 de la LOPD.

Este mensaje y sus archivos adjuntos van dirigidos exclusivamente a su destinatario, pudiendo contener información confidencial sometida a secreto profesional. No está permitida su reproducción o distribución sin la autorización expresa la Iglesia

Si usted no es el destinatario final por favor elimínelo e infórmenos por esta vía.

De acuerdo con la LOPD, le informamos que sus datos personales y dirección de correo electrónico forman parte de un fichero, cuyo responsable es la Iglesia, siendo la finalidad del fichero;⁵.

Si lo desea, podrá usted ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos enviando un mensaje a la siguiente dirección de correo electrónico a, indicando en la línea de “Asunto” el derecho que desea ejercitar.

⁵ La Iglesia deberá indicar la concreta finalidad a la que se destinarán los datos del destinatario del correo-e.