

A lo largo de 2016, **JF Protección de Datos** ha venido ayudando al **Consejo General de Colegios Oficiales de Graduados Sociales de España** para cumplir con lo establecido en la Ley Orgánica de Protección de Datos (LOPD) y, en especial, con su Reglamento de Desarrollo 1720/2007.

En este sentido y, desde entonces, estamos ayudando a mantener todo lo referente a la LOPD y su Reglamento de Desarrollo en El Consejo General.

Asimismo, ayudaremos a El Consejo General a adaptarse a los nuevos requerimientos legales Europeos de Protección de Datos que entraran en vigor a partir de 2018 y que todas las empresas españolas están obligadas a cumplir, por lo que es necesario y crítico que en el 2017 se implanten y actualicen los nuevos requisitos que establece el Reglamento General de Protección de Datos Europeo (RGPD), así como la implantación de las recomendaciones de la Agencia Española de Protección de Datos (AEPD).

La AEPD ya ha informado que, los responsables deben, ante todo, asumir e ir adaptándose a lo largo de 2017 al RGPD.

El RGPD establece importantes cambios y novedades a implantar en todas las empresas, destacando entre ellos los siguientes puntos:

- **Responsabilidad Activa:** Necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD.
- **Consentimiento Inequívoco:** Consentimiento mediante una manifestación del interesado o mediante una clara acción afirmativa, informando de una manera clara y comprensible.
- **Delegado de Protección de Datos:** Sus funciones serán las de informar y asesorar a la organización en lo referente a sus obligaciones, supervisar la implementación y aplicación de las políticas de privacidad, atender a las solicitudes de los interesados, etc.
- Disponer de un **nuevo documento de seguridad incluyendo los tratamientos** con datos de carácter personal.
- **Encargado del Tratamiento:** Recurrir únicamente a encargados que ofrezcan suficientes garantías.

- **Protección desde el Diseño y Por Defecto:** Establecer medidas técnicas y organizativas con anterioridad al inicio del tratamiento y, también, cuando se esté desarrollando.
- **Notificación de Violaciones de Seguridad:** Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, en este caso, a la AEPD.
- **Régimen Sancionador:** Aumento de las multas de hasta 20 millones de euros o el 4% de su volumen de negocios total anual.

Queremos recordarles que la falta de actualización se puede observar desde fuentes de acceso público y la propia Agencia Española de Protección de Datos, por lo que, considerando las implicaciones de imagen, así como las posibles sanciones asociadas, les recomendamos abordar la actualización y adaptación a la nueva normativa de protección de datos europea (RGPD).

Por todo ello quedamos a su disposición para comentar personalmente las implicaciones y procedimientos a realizar para adaptarse a todos los aspectos en materia de Protección de Datos.





PROTECCIÓN DE DATOS PARA COLEGIOS OFICIALES DE GRADUADOS SOCIALES DE ESPAÑA Y COLEGIADOS

1 Porqué el Colegio o Colegiado necesita la LOPD

Quizás sepa que la LOPD es un requisito obligatorio en su Colegio de Graduados Sociales (en adelante, Colegio). Es posible que incluso le haya mencionado el Consejo General de Graduados Sociales o su gestor que tenía que tener, si o si, la LOPD.

Entendemos que esto le puede significar ¿Otro gasto más? ¿Otro papeleo más? ¿Otra pérdida de tiempo?

Es casi seguro que todavía siga sin adecuar su Colegio a la LOPD.

Puede que alguien le informara de manera correcta acerca de la relevancia que tiene este trabajo de adecuación para su Colegio.

El Colegio debe enfrentarse a demasiados requisitos legales, pero la LOPD es mucho más que eso.

2 ¿Porqué adaptar su Colegio a la LOPD?

El Colegio va a disponer de datos de colegiados, clientes, proveedores, empleados, candidatos a un puesto, colaboradores, etc.

En cada caso, se recogen diferentes tipos de datos personales:

- Nombre y apellido, Dirección, teléfono, datos de pago, email, fecha de nacimiento, imágenes, etc.
- Recoges CV de candidatos, datos completos de empleados para gestión de nóminas, recursos humanos y evaluaciones.
- Datos de clientes para facturación, gestión de cobros, promociones, etc.
- Datos de usuarios de la página web.
- Datos de imágenes de videovigilancia.

Toda esa información con datos de personas relacionadas con su Colegio son de su responsabilidad.

El Colegio debe garantizar la confidencialidad de todos esos datos personales, se alimenta de esa información, son el principal activo del Colegio.

Si además, su Colegio se está desplazando hacia entornos en internet, entonces el riesgo se multiplica.

Cualquier amenaza a la confidencialidad o brecha de seguridad, significa que su Colegio no ha sabido proteger la información que almacena.

Para evitar esa situación, la LOPD será su mejor aliado, ya que gracias a unas buenas prácticas, adecuación y procedimientos podrá reforzar la seguridad de su Colegio y evitar pérdidas económicas y de imagen.

Por eso, adecuar su Colegio a la LOPD es mucho más que rellenar un formulario de inscripción para la Agencia Española de Protección de Datos.

3 Como la LOPD puede beneficiar a su Colegio de Graduados Sociales

La LOPD generará un entorno de confianza y seguridad en su Colegio que se traduce en grandes beneficios.

El beneficio mayor es saber que, pase lo que pase, podrá acreditar siempre su compromiso y diligencia con la confidencialidad de su colegiados, clientes y las personas relacionadas con su Colegio.

4 ¿Puede garantizar que cumple con la LOPD?

Es posible que estas preguntas le puedan ayudar a calificar el nivel de confidencialidad que es capaz de garantizar su Colegio a sus colegiados, clientes, colaboradores, etc.

- ¿Qué recursos ha dedicado a proteger los soportes que almacenan información personal de los colegiados, clientes y personas relacionadas con su Colegio?
- ¿Que sistema de respaldo y recuperación ha instalado en sus equipos?
- ¿Que formación tienen sus empleados para utilizar de manera segura los soportes de su Colegio? ¿Han firmado un compromiso de confidencialidad y buenas prácticas?
- ¿Que sistema de seguridad de acceso ha diseñado para limitar los accesos a la información privilegiada en su Colegio?
- ¿Cuántos de sus proveedores han firmado acuerdos de confidencialidad? ¿Cuántos disponen de una política de seguridad que proteja la información que comparte con ellos?

Si este es su caso, debe revisar todas las medidas de seguridad implementadas en su Colegio dirigidas a cumplir con la normativa vigente sobre protección de datos de carácter personal.

5 El costo de un ataque a su Colegio

Después de una fuga de datos o violación de seguridad, es necesario determinar exactamente lo que va a perder, cuánto y qué hacer al respecto.

Estas preguntas le pueden ayudar a calcular las pérdidas:

- ¿Cuánto dinero va a perder relativa a información de colegiados, clientes, etc?
- ¿Cuanto le costará en términos de desarrollo / modificación de programas?
- ¿Cuánto dinero va a perder en gastos de notificación, juicios, sanciones, auditorías y daños a la marca cuando la violación de los datos se haga pública?
- ¿Cuánto tiempo deberá invertir en identificar, abordar y recuperar todos los sistemas afectados?
- ¿Cuánto deberá abonar en concepto de infracciones si sus medidas de seguridad no cumplen con las políticas y requisitos de seguridad exigidos por la LOPD?

Por supuesto, adecuar su Colegio tiene muchas mas ventajas y la prevención es la mejor protección.

6 Quienes Somos

Somos un grupo de profesionales procedentes de las grandes consultoras, con una dilatada experiencia en el sector, que iniciaron un proyecto ambicioso con el objetivo de ofrecer una colaboración profesional que, en muchas ocasiones, habíamos realizado para los grandes clientes de las consultoras.

Viendo la dificultad que existía en las empresas para dar respuesta a la Ley Orgánica de Protección de Datos (LOPD), vimos la necesidad de ofrecer un servicio integral para poder cumplir con lo estipulado en la Ley. El nivel de conocimiento de estos servicios era elevado gracias a nuestra etapa como consultores.

Fue entonces cuando nos decidimos a crear JF Protección de Datos, una compañía dedicada, única y exclusivamente, a ofrecer a sus clientes un servicio integral, desde el asesoramiento hasta el mantenimiento pasando por la adaptación y auditoría bienal exigida por la Ley; involucrando al cliente en todas las fases del desarrollo de nuestro trabajo.

A lo largo de estos años, hemos tenido la suerte de trabajar para grandes Compañías que nos han dado la oportunidad de seguir progresando y creciendo, lo que nos ha permitido aportar un valor añadido a nuestro trabajo. La consolidación en este mercado tan competitivo viene avalada por la confianza depositada en JF Protección de Datos por nuestros clientes.

JF Protección de Datos le asegura el cumplimiento de estas obligaciones de la forma más sencilla para su empresa, poniendo a disposición de sus clientes una serie de servicios específicos relacionados con la LOPD:



JF Protección de Datos, S.L.

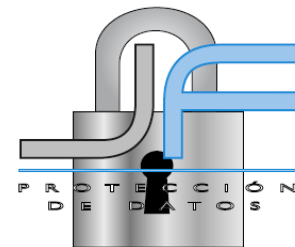
www.jfprotecciondedatos.com

info@jfprotecciondedatos.com

c/ Paseo de los Parques, 6 - 28100 - Madrid

Teléfono: 670 900 049

Nuestros servicios LOPD



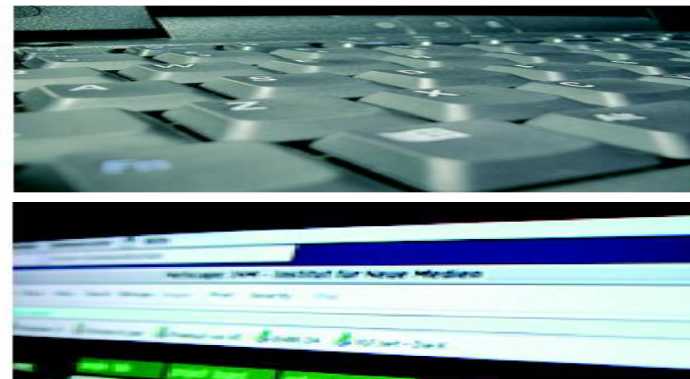
“La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”

Artículo 18.4 de la Constitución Española.

La ley afecta a “los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado” (art. 2.1), entendiendo por **datos de carácter personal**, de conformidad con las definiciones contenidas en el art. 3, “cualquier información concerniente a personas físicas identificadas o identificables”.

Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo al tratamiento de las personas físicas en lo que respecta al tratamiento de datos personales.



ASESORAMIENTO

- Orientación en:
 - Identificación, clasificación y declaración de ficheros.
 - Documento de Seguridad.
- Colaboración en la definición de roles organizativos.
- Asistencia ante procesos sancionadores.

DIAGNÓSTICO SITUACIÓN

- Identificación de los ficheros de datos de carácter personal, de su finalidad, y de su tratamiento por parte de las diferentes unidades y departamentos.
- Clasificación de los ficheros identificados según los tres niveles establecidos en la LOPD (básico, medio y alto).
- Análisis de los documentos empleados para recabar datos de carácter personal y sus coberturas formales.

ADECUACIÓN

- Colaboración en la declaración de ficheros ante la AEPD.
- Revisión de las cláusulas y contratos referentes a la LOPD.
- Revisión de las medidas de seguridad actuales de los sistemas de información en que residan los ficheros.
- Desarrollo del Documento de Seguridad.
- Desarrollo o actualización de procedimientos en el ámbito del Reglamento.

AUDITORÍA

- Diagnostico del grado de cumplimiento que exige el Reglamento y enumerar las modificaciones encaminadas a satisfacer dicho cumplimiento.
- Revisar las medidas de seguridad que actualmente están implantadas en los Sistemas de Información.
- Generar el informe de cumplimiento exigido en el Reglamento de Seguridad. Elaborar un Plan de Acción, organizativo y técnico.

MANTENIMIENTO

- Outsourcing para la Gestión de la LOPD y el Reglamento de Medidas de Seguridad.
- Adaptación permanente a la LOPD.
- Coordinar y controlar las medidas técnicas y organizativas.
- Revisiones periódicas para verificar el cumplimiento de lo dispuesto en la normativa de protección de datos.
- Definición y desarrollo de un programa de formación y concienciación del personal.
- Soporte en la reuniones periódicas del Comité LOPD en la compañía.