

Adecuación a la LOPD Protección de Datos de Carácter Personal

Situación Actual

Tradicionalmente, las personas han ido dando sus datos personales a entidades públicas y privadas, de buena fe, como al registrarse en un hotel, al ingresar en un hospital, solicitar un empleo o una tarjeta de crédito, etc, sin pensar en los efectos secundarios que esta entrega de datos pudiera originar.

El resultado ha sido una invasión de correo no deseado en nuestro domicilio para vendernos un viaje de placer, una segunda vivienda en la playa, un préstamo, etc. Más preocupante que esto puede ser que nuestros datos personales pasen a formar parte de ficheros de morosos que las instituciones consultan a efectos de concesión de créditos, o que nuestros datos de salud, situación familiar o ideología política terminen en papeleras públicas.

Para evitar este mal uso y proteger así el derecho fundamental sobre la privacidad e intimidad de las personas, se promulgó la LOPD (Ley Orgánica de Protección de Datos Personales).

Situación Deseada

El cambio de la situación tradicional a la impuesta por la legislación requiere una inversión en tiempo y dinero por parte de las empresas e instituciones. En la actualidad, las empresas e instituciones españolas aún deben esforzarse para lograr este cambio, a pesar de las sanciones económicas que la Agencia Española de Protección de Datos (AEPD) impone cuando un ciudadano acude a ella denunciando la violación de sus derechos y de que la cuantía de una sola sanción puede llegar a la cifra de 600.000 Euros.

La adecuación a la LOPD debe verse como algo continuado, que ha de cumplirse día a día.

El Reglamento que desarrolla esta Ley Orgánica lo entiende de esta manera, al obligar a una auditoría al menos cada dos años, que muestre el grado de su cumplimiento.

Nuevo Reglamento

El nuevo Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, cuya entrada en vigor se ha producido en abril de 2008, prevé una ampliación y regulación menos generalista de las obligaciones sobre protección de datos.

En concreto y entre otros aspectos, el Reglamento ha venido a:

- aclarar su ámbito objetivo de aplicación;
- establecer una regulación del modo de captación del consentimiento, por ejemplo, en el caso de los menores o de los servicios de comunicaciones electrónicas;
- prever criterios específicos para determinados ficheros de titularidad privada, como los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial;
- ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que correspondan en cada caso y en sus revisiones posteriores.
- ordenar con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del Documento de Seguridad, de obligada tenencia en las empresas.

Servicios Relativos a la LOPD

La transformación de una empresa o institución de una situación de incumplimiento de la LOPD a una situación de cumplimiento de la misma suele tener cierto grado de dificultad. Las razones pueden ser la implicación y participación de forma continuada de muchos departamentos, tales como Recursos Humanos, Jurídico, Organización, Informática, Dirección General, e incluso en muchos casos, de las empresas externas a las que se entregan datos personales para su tratamiento.

De la misma manera, esta transformación requiere la acción combinada de personal especialista en diferentes ámbitos: jurídico, informático y organizativo.

Todo esto hace que muchas empresas decidan externalizar este cumplimiento y ponerlo en manos de empresas especializadas. Si éste es su caso, ESA Security le puede ofrecer los siguientes servicios:

• Diagnóstico

Consiste en identificar las debilidades jurídicas, organizativas y técnicas de la empresa o institución, diciendo al mismo tiempo el artículo incumplido de la LOPD o del Reglamento, su grado de severidad y la acción correctora recomendada.

• Adecuación

Se realizan entrevistas con los Directores de Departamento y se solicita la documentación de las distintas áreas de la compañía. Del estudio de la documentación e información obtenida en las entrevistas se definen qué medidas de control jurídicas, técnicas y organizativas deben llevarse a cabo en la empresa para una correcta adecuación a la LOPD.

ESA Security se encarga de realizar la declaración de ficheros ante la AEPD, así como de redactar el preceptivo Documento de Seguridad, los procedimientos establecidos en el Reglamento de desarrollo de la LOPD, las cláusulas y los documentos necesarios para el cumplimiento de la normativa. En esta misma línea, se averigua si existen transferencias internacionales de datos y en caso afirmativo se recomiendan las acciones oportunas.

ESA Security entrega un documento que contiene la Definición de Medidas Técnicas y un Manual de Procedimientos Jurídicos para el cumplimiento de la normativa vigente y de acuerdo con las necesidades concretas y específicas de la organización, así como un Informe Ejecutivo en el que se recogen los aspectos que ha de tener en cuenta en la materia, atendiendo a cada una de las áreas detectadas en la organización.

• Plan de Implantación

Una vez hecha la adecuación es necesario que las medidas indicadas en el Informe Ejecutivo se lleven a la práctica. Esto es lo que se llama "la implantación", lo que a su vez exige un Plan de Implantación

ESA Security dispone de una metodología propia y específica para llevar a cabo la implantación de las medidas indicadas en el Informe Ejecutivo de una forma ágil, rápida y fiable. Mediante el uso de esta metodología podemos ofrecerle un Plan de Implantación detallado donde se desglosan y se personalizan las medidas jurídicas, técnicas y organizativas detectadas en el proceso de adecuación previo, por cada área o departamento de la organización y para cada situación del negocio en que la Ley Orgánica es aplicable.

• Bolsa de Horas

Puede contratar un número de horas de servicio que serán utilizadas a lo largo de un periodo de doce meses desde su activación. Con este servicio ya sea vía

mail o por teléfono dispondrá de un apoyo de personal especializado para resolver sus consultas.

• Mantenimiento

Este servicio está orientado a las empresas que quieren cumplir con sus obligaciones dedicando al mismo tiempo el menor tiempo posible de sus empleados. Incluye la revisión de los ficheros declarados, de los contratos, políticas y procedimientos, así como la actualización del documento de seguridad, las consultas jurídicas y la auditoría bienal.

• Revisión de Situación

Los cambios estructurales de la empresa cliente pueden hacer recomendables revisiones de la LOPD. ESA Security, a través de un informe ejecutivo, puede darle a conocer el grado de adaptación de la empresa a la Normativa de Protección de Datos verificando el cumplimiento de los controles, procedimientos e instrucciones en materia de seguridad de datos, así como todo lo contemplado en el Reglamento de Desarrollo de la LOPD.

• Auditoría

La auditoría informática es obligatoria por el Reglamento al menos cada 2 años. La auditoría establece si las medidas correctoras descritas en la adecuación se han llevado a la práctica. Por esta razón, recomendamos hacerlas con la periodicidad que marquen los cambios estructurales de la empresa.

• Planes de Formación

Mediante cursos presenciales se orienta al personal de la organización, (ya sean Directivos o Empleados) para dar a conocer las tareas y responsabilidades que les impone la normativa de la LOPD.

Beneficios

- Ganar confianza frente a los clientes, proveedores, empleados, accionistas y/o terceros.
- Eliminación de muchos riesgos propios del negocio. Durante la adecuación, re-

visión o auditoría se encuentran debilidades tales como ficheros desprotegidos que pueden ser copiados, robados o dañados, falta de procedimientos adecuados o no establecidos en el documento de seguridad, ausencia de relaciones contractuales que regularicen las cesiones o encargos de tratamiento, etc.

- Mejora de la productividad. Como consecuencia de la adecuación y auditoría, se pueden descubrir procesos innecesarios, redundantes, o ineficientes que pueden mejorarse sustancialmente con muy poco esfuerzo.

- Reducción del riesgo de sanciones. Este riesgo va en aumento a medida que el público en general va perdiendo el miedo a denunciar la lesión de sus derechos ante la Agencia Española de Protección de Datos (AEPD). Muy a menudo, son los propios empleados o ex-empleados los que ponen la denuncia.

- Reducción del riesgo de mala imagen. Cumpliendo con la LOPD, se reduce el riesgo de una mala publicidad en los medios de comunicación. Con frecuencia, esto es un factor de motivación superior a la propia sanción.

Sobre ESA Security

ESA Security es una consultora especializada únicamente en la Seguridad de la Información que realiza frecuentemente con éxito la preparación de empresas para que consigan su Certificación ISO 27001 sobre la Seguridad de la Información con cualquier certificadora acreditada por ENAC o UKAS.

Sus profesionales están altamente cualificados, incluyendo certificaciones CGEIT, CISM y CISA, y lo más importante: con la experiencia práctica de haber conseguido Certificaciones ISO 27001 y haber realizado en múltiples ocasiones Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis y Gestión de Riesgos, Proyectos de Hacking Ético, Formación en Seguridad, Adecuaciones y Auditorías LOPD y servicios relativos a la Seguridad de la Información en general.