Protección de datos

Protección legal de datos de archivos

La protección de datos personales y velar por la privacidad de la información es un tema de suma importancia a nivel de empresas y de países. El mal uso de información personal puede constituir un delito.

Algunos países han creado organismos que se encargan del tema y de legislar respecto del acceso, uso y confidencialidad de los datos.

Agencia Española de Protección de datos

Web de la Agencia

Ley de Protección de Datos de caracter personal consolidada

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de d iciembre, de protección de datos de carácter personal.

Regula derechos del usuario

Derecho de información

En el momento en que se procede a la recogida de los datos personales, el interesado debe ser informado previamente de modo expreso, preciso e inequívoco de, entre otros, la existencia de un fichero, de la posibilidad de ejercitar sus derechos y del responsable del tratamiento.

Derecho de acceso

El derecho de acceso permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento.

Regula derechos del usuario

Derecho de rectificación

Este derecho se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Derecho de cancelación

El derecho de cancelación permite que se supriman los datos que resulten ser inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD.

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 en el mismo.

Regula derechos del usuario

Derechos relacionados con el ámbito de la publicidad:

Derecho de exclusión de guías de teléfonos

Derecho a no recibir publicidad no deseada

Derechos de los abonados y usuarios de servicios de telecomunicaciones

Derechos de los destinatarios de servicios de comunicaciones electrónicas

Define obligaciones del Responsable del fichero

Inscripción de ficheros

* Notificar los ficheros ante el Registro General de Protección de Datos, para que se proceda a su inscripción.

Calidad de los datos

* Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

Deber de guardar secreto

* Garantizar el cumplimiento de los deberes de secreto y seguridad.

Define obligaciones del Responsable del fichero

Deber de información

* Informar a los titulares de los datos personales en la recogida de éstos.

* Obtener el consentimiento para el tratamiento de los datos personales.

Atención de los derechos de los ciudadanos

* Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

* Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD.

* Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.

Obtención del formulario NOTA

NOTIFICACIONES TELEMATICAS A LA AEPD

Para realizar la inscripción inicial del fichero y, en su caso, la posterior modificación o supresión de la inscripción, en la página web de la AEPD (www.agpd.es) se encuentra disponible **el formulario electrónico** a través del que deberán efectuarse, de **forma gratuita**, las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos (aprobado mediante Resolución de la AEPD de 12 de julio de 2006- B.O.E. 181 de 31 de julio).

Este formulario permite la presentación de forma gratuita de notificaciones a través de Internet con certificado **de firma electrónica.** En caso de no disponer de un certificado de firma electrónica, también puede presentar la notificación a través de Internet, para lo cual deberá remitir a la Agencia la Hoja de solicitud correspondiente al envío realizado debidamente firmada. Por último, puede optar por el modo de presentación en soporte papel.

Medidas de seguridad

El principio de seguridad de datos establecido en el artículo 9 de la Ley Orgánica 15/1999, impone al responsable del fichero 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. Estas medidas han sido desarrolladas en el Título VIII del Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Artículo 9. Seguridad de los datos.

"El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán 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, ya provengan de la acción humana o del medio físico o natural.
No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El artículo 8o del RDLOPD señala que las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto y, a continuación, el artículo 81 especifica la aplicación de los niveles de seguridad según el tipo de datos de carácter personal a tratar. Por último señalar que el responsable encontrará en el artículo 88 la concreción del contenido del documento de seguridad, y por tanto, un índice de ayuda para llevar a cabo su construcción.

Con el objeto de facilitar a los responsables de los ficheros la adopción de las disposiciones del Reglamento de Seguridad, se ha elaborado un modelo de "documento de seguridad", que puede servir de guía en el desarrollo de las previsiones del Real Decreto.

El reglamento de desarrollo de la LOPD ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Así, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Guía de seguridad de Datos

Modelo de documento de seguridad

Se definen **niveles de seguridad**, englobando cada uno al anterior como si se tratara de un sistema de capas concéntricas donde la más alta contiene a la inferior. El nivel de seguridad del fichero concuerda con la importancia de su información, puede ser:

.-**Básico:** se aplica a todos los ficheros que contienen datos de carácter personal.

.-**Medio:** contienen, además, información sobre cuestiones administrativas, penales, hacienda pública, servicios financieros o cuando varios datos en su conjunto permitan obtener el perfil de un individuo.

.-**Alto:** contiene datos (al menos uno) relacionados con la ideología, religión, orientación sexual o política, salud, datos policiales obtenidos sin consentimiento o cualquier otro que, si fuera conocido, dañaría principios fundamentales.

Medidas de seguridad de nivel básico:

- Elaboración del Documento de Seguridad
- Plan de incidencias y registro de las mismas
- Identificación y autentificación de los usuarios
- Control de accesos
- Gestión de soportes
- Protocolos de copias de seguridad

Medidas de seguridad de nivel medio:

•Documento de Seguridad (más requisitos que el anterior)
•Responsable de seguridad (obligatorio, pero no sustituye ni reemplaza al responsable del fichero)
•Auditorías (externas o internas)
•Plan de incidencias y registro de las mismas
•Identificación y autentificación de los usuarios
•Diseño de sistemas de control
•Gestión de soportes
•Protocolos de copias de seguridad
•Pruebas con datos ficticios o con altas medidas de seguridad

Medidas de seguridad de nivel alto:

- Documento de Seguridad (el de máximo nivel de seguridad)
- Responsable de seguridad
- Auditorias (externas o internas)
- Plan de incidencias y registro de las mismas
- Identificación y autentificación de los usuarios
- Diseño de sistemas de control
- Distribución de soportes y encriptación para transporte de datos
- Copias de seguridad en lugares físicos diferentes. Encriptación
- Encriptación de datos a través de las redes

Búsqueda ficheros inscritos

Búsqueda de ficheros de Titularidad Pública: Resultado

Se han encontrado 8 ficheros.

Tipo de Administración: ADMON. Y ORGANISMOS PÚBLICOS DE C. AUTONOMAS
Comunidad Autónoma: COMUNIDAD DE MADRID
Responsable: CONSEJERIA DE EDUCACION
DIRECCION AREA TERRITORIAL MADRID CAPITAL
C P LOS ALMENDROS

Nombre del fichero: **ALUMNOS**
Finalidad: EXPEDIENTE ACADEMICO DE LOS ALUMNOS Y GESTION Y SEGUIMIENTO DEL EXPEDIENTE ACADEMICO DE LOS ALUMNOS DEL CENTRO ADMISION DE ALUMNOS

Nombre del fichero: **EXPEDIENTE ACADEMICO**
Finalidad: EXPEDIENTE ACADEMICO DE LOS EX ALUMNOS Y GESTION Y SEGUIMIENTO DEL EXPEDIENTE ACADEMICO DE LOS ALUMNOS DEL CENTRO ADMISION DE ALUMNOS Y GESTION DE BECAS

Nombre del fichero: **MAESTROS**
Finalidad: GESTION Y CONTROL DEL PERSONAL DOCENTE

Búsqueda de ficheros de Titularidad Privada: Resultado

RAZON SOCIAL FRED OLSEN S A

Nombre del fichero: **CLIENTES Y/O PROVEEDORES**
Finalidad: GESTION DE CLIENTES Y/O PROVEEDORES

Nombre del fichero: **MARKETING Y PUBLICIDAD**
Finalidad: ENVIO DE INFORMACION COMUNICACIONES COMERCIALES ACTIVIDADES Y/O EVENTOS

Nombre del fichero: **NOMINAS PERSONAL Y RECURSOS HUMANOS**
Finalidad: GESTION DE NOMINAS Y RECURSOS HUMANOS

Nombre del fichero: **VIDEOVIGILANCIA**
Finalidad: VIDEOVIGILANCIA DE LAS INSTALACIONES

Las listas Robinson permiten que las personas anoten en ellas teléfonos o direcciones en las cuales no quieren recibir información publicitaria. El compromiso de los grandes generadores de campañas publicitarias es consultarlas para excluir de ellas a los allí anotados.

https://www.listarobinson.es/

Reforma de la protección de datos – Nuevas reglas adaptadas a la era digital

Entre otras disposiciones, las nuevas reglas incluyen:

- el derecho al “olvido”, mediante la rectificación o supresión de datos personales,
- la necesidad de “consentimiento claro y afirmativo” de la persona concernida al tratamiento de sus datos personales,
- la “portabilidad”, o el derecho a trasladar los datos a otro proveedor de servicios,
- el derecho a ser informado si los datos personales han sido pirateados,
- lenguaje claro y comprensible sobre las cláusulas de privacidad, y
- multas de hasta el 4% de la facturación global de las empresas en caso de infracción.

El nuevo delito de acceso ilícito a datos o programas informáticos (art. 197.3 Código Penal)

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. **Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos** y a quien los altere o utilice en perjuicio de titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Caso Facebook: golpe al envío de datos personales de usuarios a EEUU

http://estaticos.expansion.com/opinion/documentosWeb/2015/10/06/sentenciafacebook.pdf

Se denunció el envío de datos personales desde los servidores irlandeses de Facebook, donde la compañía ha fijado su sede europea, a los que tiene en EEUU, al considerar que el país americano no garantizaba sus derechos. El ciudadano austriaco inició su proceso después de que el ex empleado de la Agencia Central de Inteligencia de EEUU (CIA), Edward Snowden, desvelara en 2013 que los servicios de información estadounidenses tenían acceso a estos datos.

El Tribunal de Luxemburgo sostiene que EE UU no garantiza “un nivel de protección adecuado” de la información transferida desde Europa

Todas aquellas empresas que utilicen plataformas tecnológicas que realicen transferencias de datos de ciudadanos europeos a terceros países (incluido EEUU), como por ejemplo Dropbox, Google Drive o MailChimp, tienen hasta el 29 de enero de 2016 para cumplir con la nueva normativa o ser multadas.

De esta forma, la AEPD ha requerido a todas las compañías para que dejen de usar estos servicios salvo que cumplan una de estas tres opciones: contar con la autorización del Director de la Agencia, el consentimiento informado de todas las personas cuyos datos se vean afectados o utilizar alguna de las excepciones previstas en el artículo 34 de la Ley Orgánica 15/1999, como lo puede ser por ejemplo realizar una transferencia para auxilio judicial o un diagnóstico médico.