AIG

BusinessGuard DataPlus

Guía para mediadores

Seguro de Responsabilidad por Protección de Datos Personales

Todas las empresas tratan datos de carácter personal, ya sea de sus propios empleados, de sus clientes o de potenciales consumidores.

No sólo nombre y apellidos son datos considerados como personales sino que existe otra mucha información que permite identificar a las personas y que puede ser considerada dentro de la categoría de datos personales, como es el caso de fotografías o imágenes, la voz, la huella digital, la dirección postal o de correo electrónico, la fecha de nacimiento, o combinaciones numéricas como el número de teléfono, el de la Seguridad Social, el de identidad (DNI) o el de identificación fiscal (NIF), etc... Todo ello sin contar con aquellos especialmente protegidos por ley como son los relativos al origen racial, la salud o la vida sexual o que revelen la ideología, religión, creencias, o afiliación sindical de la persona.

En la actualidad, las empresas deben desenvolverse en un entorno altamente exigente en materia de protección de datos personales. Las empresas deben tomar una actitud cada vez más vigilante ante nuevas y mayores obligaciones a las que se debe dar escrupuloso cumplimiento, y ante el riesgo de incurrir en responsabilidades por infracciones que adicionalmente pueden dar lugar a inspecciones de autoridades administrativas, cuyo fin es velar por el cumplimiento normativo y que pueden llegar a imponer sanciones administrativas.

Más allá del impacto económico de posibles indemnizaciones por daños y perjuicios o sanciones a las que deba hacer frente una empresa, una infracción del uso confidencial de datos de carácter personal puede dañar seriamente uno de los valores más preciados de la empresa, su reputación, con el consecuente desgaste de su imagen y posible pérdida de clientes u oportunidades de negocio.

Un Entorno Cambiante

En España recientemente se ha regulado con más detalle la protección de datos personales, con la aparición en enero de 2008 del Reglamento de Protección de Datos, que amplia la normas vigentes desde la aparición de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, también conocida por sus siglas **LOPD**.

Las autoridades legislativas españolas y de gran parte del extranjero han reaccionado rápidamente para establecer un estándar mínimo de protección al ciudadano.

- En ESPAÑA, la protección de los datos de carácter personal ha sido reconocida como un derecho fundamental por la Constitución y por el propio Tribunal Constitucional. Se ha desarrollado una de las normativas más estrictas existentes en la actualidad, con una activa participación de la Agencia de Protección de Datos que vela por su cumplimiento.
- En el resto de la UNIÓN EUROPEA se armonizan similares niveles de elevada protección gracias a la Directiva Europea 95/46/CE, transpuesta por los diferentes estados miembros.
- En el RESTO DEL MUNDO la preocupación no es menor y nuestra Agencia de Protección de Datos considera entre otros a Canadá, Noruega, Suiza, Argentina o Estados Unidos de América (a través de la adhesión a los “principios del puerto seguro”) como países en los que existen niveles adecuados de protección.

Claves de la protección de datos personales

Los principales sujetos relacionados con la protección de datos personales son:

- El RESPONSABLE DEL FICHERO O TRATAMIENTO: Persona o entidad que decide sobre la finalidad, contenido y uso del tratamiento.
- El AFECTADO O INTERESADO: Persona titular de los datos personales.
- El ENCARGADO DE TRATAMIENTO: Persona o entidad que trata los datos por cuenta del responsable.

Los principios esenciales que vertebran la de datos personales son:

- La CALIDAD de los datos:
  1. Los datos personales serán recogidos por medios **leales** y **lícitos**.
  2. Los datos personales sólo podrán recogerse y tratarse cuando sean **adecuados**, **pertinentes** y **no excesivos**.
  3. Los datos personales deben recogerse con **fines determinados**, **explícitos** y **legítimos** y no deben ser tratados para otros fines.
  4. Los datos personales deberán ser **exactos** y deberán de mantenerse **actualizados** para que respondan con veracidad a la situación del titular.
  5. Los datos personales no deberán de ser mantenidos más **tiempo** del **necesario**.
  6. Los datos personales sólo podrán ser tratados **respetando los derechos** de los titulares de los mismos.
  7. Los datos personales deberán ser **protegidos** con medios técnicos y materiales apropiados de seguridad para evitar accesos no autorizados.
  8. Los datos personales no deberán ser **transmitidos** fuera del Espacio Económico Europeo (EEE) a no ser que el país de destino tenga un nivel adecuado de protección, cuyo estándar determina la Agencia Española de Protección de Datos.

- El DEBER DE INFORMACION en la recogida de los datos:

Los titulares de datos personales deberán, en términos generales, ser informados en el momento de la recogida de sus datos acerca de:

1. La existencia de un fichero.
2. La finalidad para la que se utilizan sus datos.
3. Sus derechos de acceso, rectificación, cancelación u oposición.
4. La identidad y dirección del responsable del fichero en el que se incluyen sus datos.

- El CONSENTIMIENTO PARA EL TRATAMIENTO de los datos:

El tratamiento de los datos requerirá, en términos generales, que el consentimiento del afectado sea inequívoco (ya sea otorgado de forma expresa o tácita en función de los casos) pudiendo ser el mismo revocado en cualquier momento con causa justificada para ello.

El consentimiento deberá ser **expreso** y **escrito** cuando se trate de datos relativos a ideología, religión, creencias y afiliación sindical.

El consentimiento deberá ser **expreso**, aunque no necesariamente escrito, cuando sean datos relacionados con la salud, el origen racial y la vida sexual.

En el caso de los afectados menores de edad, si el titular no alcanza los catorce años se requerirá el consentimiento de los padres o tutores.

El riesgo por protección de datos personales

¿Qué empresas están expuestas a esta clase de riesgos? La única respuesta válida es: **todas**. Un simple error, una falta en un procedimiento, un quebranto en la seguridad, el comportamiento indebido de un empleado, o la ausencia de una persona clave de la organización pueden acarrear consecuencias económicas graves a la empresa.

No obstante lo anterior hay empresas que por la naturaleza de su negocio tienen mayor contacto con los ciudadanos de a pie y en consecuencia tienen mayor exposición al riesgo.

Los sectores de actividad empresarial en los que existe mayor sensibilización son: sanitario, ocio, hostelería, medios de comunicación y telecomunicaciones, transporte de viajeros, educación, publicidad, telemarketing o "call centers", servicios profesionales, proceso de datos, etc...

Responsabilidad por protección de datos

La LOPD recuerda el derecho del afectado a ser indemnizado por daños y perjuicios a raíz de incumplimientos en la protección de datos de carácter personal, acudiendo al régimen general de responsabilidad.

Las empresas deben ser conscientes de que no sólo se les podrá responsabilizar por daños derivados de su incumplimiento, sino también por los que se deriven de acciones u omisiones del encargado de tratamiento de datos, que siendo ajeno a la empresa pueda ser subcontratado para determinados trabajos de tratamiento de datos de esta naturaleza.

Conviene en todo caso no olvidar que gran número de reclamaciones no provienen de clientes sino que se producen dentro de la propia organización. Las empresas almacenan un elevado volumen de datos personales, ya sea de empleados o de candidatos a empleo, que deben ser correctamente tratados y custodiados de forma escrupulosa para garantizar su confidencialidad.

La encuesta del CIS de febrero 2008 a ciudadanos sobre protección de datos personales resaltaba como:

- **Más del 70% se muestran preocupados por su adecuado uso y protección.**
- **El 34% acudiría al juzgado y el 12% a asociaciones de defensa para denunciar usos no autorizados.**
- **Más del 50% conoce la existencia de una ley específica que protege sus derechos.**

Inspecciones y procedimientos administrativos

En España la Agencia de Protección de Datos es la encargada de velar por el cumplimiento de las normas de protección de los datos de carácter personal, y para ello ejerce la potestad inspectora y sancionadora.

La Agencia, al inspeccionar, puede requerir información, emplazar al envío o exhibición de documentos, e incluso llevar a cabo el exámen de los locales y sistemas de una empresa.

Asimismo puede sancionar ante incumplimientos. La LOPD incluye tres categorías de sanciones:

- Leves de hasta 60.101,21 Eur (Por ejemplo, no proporcionar información necesaria a los afectados en el proceso de recogida de datos).
- Graves de hasta 300.506,05 Eur (Por ejemplo, no realizar el documento de seguridad).
- Muy Graves de hasta 601.012,10 Eur (Por ejemplo, no formalizar por contrato la relación con el encargado del tratamiento de datos).

Preguntas frecuentes sobre protección de datos personales 5 aspectos a tener en cuenta en su visita al cliente

1 ¿Cómo aborda su cliente la protección de los datos personales?

La empresa, como responsable de los ficheros y del tratamiento de los datos, responde del contenido y del uso de los mismos.

Al responsable del fichero le corresponde velar por el cumplimiento de la Ley y asume obligaciones concretas como son:

- Notificar los ficheros ante el Registro General de Protección de Datos.
- Asegurarse que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a su finalidad.
- Garantizar el cumplimiento de los deberes de secreto y seguridad.
- Informar a los titulares de los datos personales en la recogida de los mismos y obtener su consentimiento para su tratamiento.
- Facilitar y garantizar los denominados derechos A.R.C.O. (acceso, rectificación, cancelación y oposición)
- Asegurarse que en su relación con terceros que le presten servicios que implique el acceso a datos personales se cumpla lo dispuesto en la Ley.

Los ficheros de datos personales no sólo son los automatizados, sino también aquellos que no estándolo permitan acceder sin esfuerzos desproporcionados a los datos de carácter personal.

Las empresas pueden incurrir en responsabilidad e incluso tener que hacer frente a procedimientos sancionadores ante incumplimientos de los requerimientos normativos.

Los plazos de Derechos A.R.C.O. son breves:

- Acceso: 1 mes para contestar y 10 días permitir acceso
- Rectificación: 10 días para corregir inexactitudes.
- Cancelación: 10 días para borrarlos o suprimirlos
- Oposición: 10 días para cesar en el tratamiento.

2 ¿Subcontrata su cliente los servicios de encargados de tratamientos de datos para desarrollar determinados aspectos de su actividad?

Al subcontratista, ya sea persona física o jurídica, se le denomina en este caso "encargado de tratamiento" por tratarse de la persona que asume el tratamiento de los datos por cuenta del responsable del fichero.

Dado que el encargado de tratamiento es **ajeno a la organización del responsable del fichero**, la Ley establece que la relación debe formalizarse por medio de contrato (por escrito o cualquier otra forma que permita acreditar su celebración y contenido) estableciendo que el encargado tratará los datos única y exclusivamente para el fin marcado sin comunicarlos a terceros.

Las empresas pueden incurrir en responsabilidad tanto por actos propios como por el comportamiento del encargado de tratamiento de datos. Ambos, el encargado de tratamiento y el responsable pueden ser sancionados de acuerdo a la LOPD si incumplen sus obligaciones.

El empleado, cuando tenga acceso a los datos en el marco de su relación laboral con el responsable del fichero, no será considerado encargado de tratamiento.

3 ¿Es adecuado el nivel de seguridad ?

El responsable del fichero y el encargado de su tratamiento deberán adoptar las **medidas técnicas** y **organizativas** necesarias para garantizar la seguridad de los datos de carácter personal y evitar su pérdida, alteración, o el acceso o tratamiento no autorizado de los mismos.

La seguridad de los datos es requisito previo para garantizar la **confidencialidad**, **integridad** y **disponibilidad** de los mismos y es necesaria tanto en todos los ficheros o tratamientos de datos personales, ya sean automatizados o no.

No obstante existen tres niveles de seguridad conforme a la LOPD:

- Nivel Alto: Ficheros que contengan datos especialmente protegidos.
- Nivel Medio: Ficheros que contengan datos relativos a infracciones administrativas o penales, Hacienda Pública, servicios financieros, solvencia patrimonial o crédito.
- Nivel Básico: Cualquier otro fichero que contenga datos de carácter personal.

El reciente Reglamento de Protección de Datos Personales ha detallado las medidas a implantar para garantizar la seguridad en los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento.

La falta de medidas de seguridad puede fácilmente derivar en responsabilidades y sanciones.

¡ La Agencia Española de Protección de Datos ha publicado en Abril 2008 una Guía de Seguridad !

Puede consultarla a través del link que facilitamos al final de la presente Guía.

4 ¿Está preparado su cliente para atender una inspección o procedimiento administrativo que pudiera derivar en sanción?

Las empresas al adoptar las medidas para cumplir con la normativa de protección de datos personales toman conciencia del importante papel que juega la Agencia de Protección de Datos al velar por su cumplimiento.

Cuando la Agencia inicia inspecciones o procedimientos, ya sea de oficio o a raíz de una denuncia, las empresas necesitan invertir recursos y esfuerzos para atender adecuadamente a las mismas. Asimismo, generalmente se precisa un asesoramiento adecuado de profesionales expertos en la materia, lo que conlleva un coste que puede alcanzar cifras considerables.

5 ¿Es consciente su cliente del daño que una falta de protección de los datos personales pueda ocasionar a su imagen? ¿Cree que sabría cómo reaccionar?

Las empresas invierten mucho tiempo y esfuerzos en construir su reputación en el mercado, pero la imagen es un valor muy frágil que puede quedar dañado o destruido en cuestión de segundos.

Una reclamación alegando una indebida protección de la confidencialidad de los datos de carácter personal que trata la empresa, puede tener un efecto devastador y prolongado en la imagen de la compañía llegando a repercutir en su cuenta de resultados.

Saber gestionar adecuadamente estas situaciones y contar con el asesoramiento especializado preciso es crítico para salvaguardar la reputación, tanto de la empresa como de los profesionales clave que forman parte de su organización.

Normativa legal básica en España

• Ley Orgánica de Protección de Datos (LOPD)

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

• Reglamento de Protección de Datos (RPD)

Real Decreto 1720/2007, de 21 de diciembre, de Protección de Datos de Carácter Personal

Acceso a información de utilidad en internet

Agencia Española de Protección de Datos (www.agpd.es)

Preguntas más frecuentes:

https://www.agpd.es/portalweb/canalciudadano/preguntasciudadano/index-ides-idphp.php##

Guía del documento de seguridad:

https://www.agpd.es/portalweb/canalresponsable/guia_documento/index-ides-idphp.php

Guía del responsable del fichero:

https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

Legislación:

https://www.agpd.es/portalweb/canaldocumentacion/legislacion/index-ides-idphp.php

Comisión Europea – Protección de Datos

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

MADRID
Paseo de la Castellana, 216
28046 Madrid
Tlfno: 91.567.74.00

BARCELONA
Avda. Diagonal, 618 – 9º A y B
08021 Barcelona
Tlfno: 93.452.28.60

BILBAO
Gran Via, 19 – 21 2ª Planta
48001 BILBAO
Tlfno: 94.470.64.50.

SEVILLA
Plaza Ruíz de Alda, 11
41004 Sevilla
Tlfno: 95.436.93.07

VALENCIA
C/ Moratín 17 - 2
46002 Valencia
Tlfno: 96.112.45.42

AIG Europe S.A.
Paseo de la Castellana, 216
Torre Este de Puerta Europa, 3ª planta
28046 – Madrid

Tlfno: 91.567.74.00