Boletín de noticias LOPD

Temas de actualidad en protección de datos de carácter personal y privacidad.

Boletín nº19 - Mayo 2013

CONTENIDOS

INTRODUCCIÓN

En esta nueva edición del « **Boletín LOPD** », MAZARS quiere poner el foco en un tema de actualidad « **El nuevo Reglamento Europeo de Protección de Datos Personales** », para conocer las principales novedades que aparecen en la propuesta publicada y pendiente de votación por los países.

Además, os proponemos una serie de **bibliografía** útil en materia LOPD, así como **blogs y webs** de consulta para manteneros al día en cuanto a interpretaciones, eventos y sentencias relacionadas con la LOPD.

Por otra parte, los próximos meses disminuye la actividad y es un excelente período para el análisis y para que las organizaciones se preparen a posibles cambios. **¿Por qué no autoevaluarnos y tratar de transformar lo que no nos gusta?** Desde nuestra experiencia queremos presentaros soluciones para mejorar el buen gobierno, adecuaros a las exigencias regulatorias, y **gestionar los riesgos implantando un modelo de autoevaluación del control interno**.

NUEVOS CONCEPTOS

A continuación introducimos una serie de conceptos que creemos es necesario empezar a manejar antes de la entrada en vigor del nuevo Reglamento europeo:

- **Autoridad de control:** es la autoridad pública establecida por un Estado miembro de acuerdo con el artículo 46. En nuestro caso la actual Agencia Española de Protección de Datos.
- **Establecimiento principal:** en lo que se refiere al responsable del tratamiento, es el lugar de su establecimiento en la Unión en el que se adopten las decisiones principales en cuanto a los fines, condiciones y medios del tratamiento de datos personales. Si no se adopta en la Unión decisión alguna en cuanto a los fines, condiciones y medios del tratamiento de datos personales, el establecimiento principal es el lugar en el que tienen lugar las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del responsable del tratamiento en la Unión. Por lo que respecta al encargado del tratamiento, por «establecimiento principal» se entiende el lugar de su administración central en la Unión.
- **Violación de datos personales:** se refiere a toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma.
- **Normas corporativas vinculantes:** son las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro de la Unión para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un Grupo de empresas.

I.REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

En Enero de 2012 se publicó la propuesta de Reglamento del Parlamento Europeo y del consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y que se puede descargar en la web de la Comisión Europea (http://ec.europa.eu/justice/data-protection/index_es.htm). Tras su aprobación este Reglamento General de Protección de Datos, sustituirá a la actual Directiva 95/46.

Este nuevo Reglamento pretende establecer un marco jurídico más sólido y coherente en materia de protección de datos en la UE, que mediante una aplicación estricta unifique la aplicación de la política de protección de datos en los países miembros. Además, pretende dar respuesta a los retos abiertos por la tecnología debido al incremento de los intercambios y recogidas de datos de hoy en día, y que permita generar confianza en el entorno en línea, siendo esto esencial para el desarrollo económico.

Entrará en vigor 21 días después de su publicación en el *Diario Oficial de la Unión Europea,* y deberá adoptarse máximo 2 años después de dicha fecha. Por lo que si consideramos que su fecha tope de aprobación es de Mayo de 2014, a mediados de 2016 todas las empresas españolas que traten datos de carácter personal deberán haber implementado estos nuevos requerimientos no considerados por nuestra actual legislación.

A continuación, expondremos las novedades de mayor relevancia que han aparecido en esta propuesta de Reglamento, pendiente de aprobación.

PRINCIPALES NOVEDADES

En cuanto a las novedades que introduce esta propuesta de reglamento, hemos querido destacar las siguientes:

El **ÁMBITO DE APLICACIÓN TERRITORIAL** cambia y no se restringe únicamente a las organizaciones que se encuentran dentro de la Unión Europea, sino que, el reglamento será de aplicación al tratamiento de datos personales en un establecimiento del responsable o del encargado del tratamiento dentro de la Unión, al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable de tratamiento no establecido en la Unión, cuando sus actividades se centren en la oferta de bienes o servicios a dichos interesados en la Unión o en el control de su conducta. Así como para el tratamiento de datos personales por parte de un

responsable del tratamiento que no esté establecido en la Unión sino en un lugar en que sea de aplicación la legislación nacional de un Estado miembro en virtud del Derecho internacional público.

El **CONSENTIMIENTO DEL INTERESADO**, se debe dar de forma explícita por cualquier medio apropiado que permita la manifestación libre, específica e informada de la voluntad del interesado. Será el responsable del tratamiento el encargado de probar que el interesado ha dado su consentimiento para un tratamiento específico.

La **ATENCIÓN DE LAS SOLICITUDES DE EJERCICIO DE DERECHOS** de los afectados, así como las medidas adoptadas a raíz de las mismas deberán ser gratuitas como hasta ahora. Sin embargo, se abre la posibilidad de que el responsable establezca una tasa, siempre y cuando pueda demostrar que son solicitudes manifiestamente excesivas por su carácter repetitivo.

Se han establecido nuevos derechos para los interesados. Así el **DERECHO AL OLVIDO** establece que el responsable de tratamiento que haya hecho públicos los datos personales deberá suprimirlos y se abstendrá de darles difusión cuando: a) los datos ya no son necesarios para los fines para los que fueron recogidos; b) el interesado retira el consentimiento en que se basa el tratamiento, o ha finalizado el plazo de conservación autorizado; c) el interesado ha ejercitado su derecho de oposición al tratamiento; d) el tratamiento de datos no es conforme con el Reglamento. Además el responsable del tratamiento deberá informar a los terceros que estén tratando dichos datos de que se ha solicitado su supresión. Por otro lado, el **DERECHO A LA PORTABILIDAD DE LOS DATOS** establece que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado podrá obtener una copia de los datos en dicho formato electrónico, así como tendrá derecho a transmitirlos a otro sistema en un formato comúnmente utilizado. Y por último el **DERECHO A OPONERSE A LA CREACIÓN DE PERFILES**, considerado como evaluar de manera automatizada aspectos personales de las personas físicas o analizar o predecir en particular su rendimiento profesional, su situación económica, su localización, su estado de salud, sus preferencias personales, su fiabilidad o su comportamiento.

El responsable de tratamiento deberá implementar **MECANISMOS DE VERIFICACIÓN** de la eficacia de las políticas y medidas obligadas por el Reglamento (documentación, medidas de seguridad, evaluaciones de riesgo, evaluaciones de impacto, autorizaciones y consultas previas y existencia del delegado de protección de datos). Siempre que no sea desproporcionado, estas verificaciones serán llevadas a cabo por auditores independientes internos o externos.

La **DOCUMENTACIÓN** que tanto el responsable como el encargado de tratamiento tendrán que conservar, en el caso de empresas u organizaciones que empleen a más de 250 personas y que no traten los datos personales solo como actividad accesoria, se compone de lo siguiente: a) Identificación y contacto del responsable, corresponsable o coencargados de los tratamientos; b)Identificación y contacto del delegado de protección de datos; c) Fines del tratamiento (intereses legítimos perseguidos); d) Descripción de las categorías de interesados y datos personales de los mismos; e) Destinatarios o categorías de destinatarios a los que se comuniquen datos personales; f) Las transferencias a terceros países u organizaciones internacionales y la documentación de garantías apropiadas si corresponde; g) Indicación general de los plazos establecidos para la supresión de las diferentes categorías de datos; h) Descripción de los mecanismos de verificación de políticas y medidas.

El Reglamento indica que tras una **EVALUACIÓN DE LOS RIESGOS**, el responsable o el encargado del tratamiento adoptarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en relación con los riesgos que entrañe el tratamiento y la naturaleza de los datos personales a proteger. Sin embargo, no hace mención expresa a las medidas a implantar como son las actualmente recogidas en el Título XIII del actual Reglamento de desarrollo de la Ley Orgánica 15/1999 (RLOPD).

A partir de la entrada en vigor de este Reglamento se deberán **NOTIFICAR LAS VIOLACIONES DE LOS DATOS PERSONALES** a la autoridad de control documentándolo debidamente, en un plazo máximo de 24 horas después de tener constancia de la misma. Por lo tanto, los encargados de tratamiento alertarán e informarán de dichas violaciones a los responsables de tratamiento para poder cumplir con la obligación. Adicionalmente, siempre que lo requiera la autoridad

de control o cuando sea probable que la violación de datos personales afecte negativamente a la protección de los datos personales o a la privacidad del interesado, también se comunicará al interesado dicha violación.

La obligación de notificar el tratamiento de datos personales a las autoridades de control quedará eliminada. Sin embargo a partir de la entrada en vigor del Reglamento, antes del tratamiento se deberá llevar a cabo una **EVALUACIÓN DE IMPACTO DE LA PROTECCION DE DATOS** siempre que el tratamiento entrañe riesgos específicos para los derechos y libertades de los interesados, es decir:

- Se hagan evaluaciones sistemáticas y exhaustivas que permitan predecir la situación económica, localización, estado de salud, preferencias personales, comportamiento.
- Se traten a gran escala datos de nivel alto
- Se haga seguimiento a gran escala de zonas de acceso público, en particular con dispositivos de videovigilancia.
- El tratamiento a gran escala de datos de niños, datos genéticos o biométricos.
- Otras operaciones que necesiten autorización previa de la autoridad de control.

Las transferencias de datos personales a terceros países u organizaciones internacionales deberán ser autorizadas por la autoridad de control como hasta ahora. Pero además se deberá **CONSULTAR A LA AUTORIDAD DE CONTROL** antes de comenzar el tratamiento de datos personales cuando la evaluación del impacto de la protección de los datos indique que es probable que las operaciones de tratamiento entrañan un elevado nivel de riesgos específicos o que las operaciones de tratamiento estén dentro de la lista publicada por la autoridad de control como operaciones de tratamiento que entrañan riesgos específicos para los derechos y libertades de los interesados.

La autoridad u organismos públicos, las empresas de más de 250 personas o las empresas cuyas principales actividades consistan en operaciones de tratamiento que requieran un seguimiento periódico y sistemático de los interesados, deberán designar un **DELEGADO DE PROTECCIÓN DE DATOS** por un mandato mínimo de 2 años. Los grupos de empresas podrán nombrar un delegado único.

También se establece que los Estados miembros y la Comisión promoverá la creación de mecanismos de **CERTIFICACIÓN** en materia de protección de datos y de **SELLOS Y MARCADORES DE PROTECCIÓN DE DATOS** que permita a los interesados evaluar rápidamente el nivel de protección que ofrecen los responsables y encargados de tratamiento.

Otra novedad dentro del reglamento viene de la mano de las **SANCIONES ADMINISTRATIVAS**. Estas han variado en su cuantía según la gravedad de la infracción:

- Leve: Multa de hasta 250.000 euros o para empresas hasta el 0,5% de su volumen de negocios anual a nivel mundial.
- Grave: Multa de hasta 500.000 euros o para empresas hasta el 1% de su volumen de negocios anual a nivel mundial.
- Muy Grave: Multa de hasta 1.000.000 euros o para empresas hasta el 2% de su volumen de negocios anual a nivel mundial.

II.BIBLIOGRAFÍA LOPD

A continuación incluimos una bibliografía práctica que nos permitirá profundizar nuestros conocimientos y resolver dudas acerca de la legislación vigente de protección de datos personales:

Estudio práctico sobre la protección de datos de carácter personal.

Autor: Ana Marzo, Cristina Almuzara, Fanny Coudert y Yolanda Navalpotro

Editorial: Lex Nova, 2007

Este libro analiza las implicaciones legales que se derivan de la normativa en materia de protección de datos para que el lector, además de adquirir un conocimiento completo sobre sus derechos y obligaciones en esta materia, sepa cómo llevarlos a la práctica.
El libro incluye numerosos ejemplos de actuación de los responsables y encargados del tratamiento, así como abundante jurisprudencia y las recomendaciones y mejoras para que los responsables de ficheros adapten sus procesos a la normativa, de acuerdo con las últimas memorias de la Agencia Española de Protección de Datos.

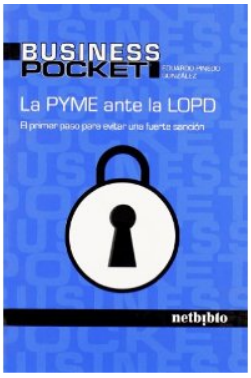
Legislación de Protección de Datos. Segunda Edición

Autor: José Luis Piñar

Editorial: Iustel, Portal de Derecho, S. A. 2.011

Elaborado por José Luis Piñar, exdirector de la Agencia Española de Protección de Datos, esta segunda edición recoge las implicaciones de la Ley de Economía Sostenible.

Además, incluye las más importantes instrucciones publicadas por la Agencia Española de Protección de Datos (por ejemplo la relativa al acceso a los edificios, o la relativa a la intimidad de los datos personales recogidos en la contratación de un seguro de vida conjuntamente con un préstamo hipotecario).



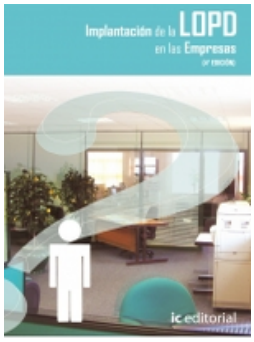
La Pyme Ante la LOPD.

Autor: Eduardo Pinedo González

Editorial : Netbiblo, S.L. 2007

La obra contenida en este libro pretende que las entidades privadas, que requieran tratar datos de carácter personal, tengan una guía que recoge de forma clara y precisa las principales obligaciones que deben tener en cuenta respecto al tratamiento de estos datos. Hoy en día es importante el cumplimiento con las obligaciones que se derivan de la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a los efectos de evitar importantes sanciones por parte de la Agencia Española de Protección de Datos.

Implantación de la LOPD en las empresas



Autor: Silvia Montero Martín

Editorial: IC Editorial, 2013

Con este libro podremos reconocer y aplicar los procesos prácticos para la implantación y adecuación de la normativa vigente de protección de datos personales (LOPD) en las empresas.

III. ENLACES DE INTERÉS

En este apartado vamos a recomendar algunos enlaces de interés y blogs que nos permitirán estar al día sobre toda la actualidad referente a la protección de datos personales:

Para descargar el Reglamento General de Protección de Datos:

- http://ec.europa.eu/justice/data-protection/index_es.htm

Estudio de impacto y comparativa con la normativa española de la propuesta de Reglamento General de Protección de Datos de la Unión Europea del Data Privacy Institute:

- https://www.ismsforum.es/noticias/noticia.php?idnoticia=386

Protección de datos personales (Samuel Parra): Blog especializado en protección de datos:

- http://www.samuelparra.com/

Universo LOPD: tu blog de protección de datos:

- http://fjaviersempere.wordpress.com/

Blog: Privacidad Lógica:

- http://www.privacidadlogica.es/

Ayuda ley Protección de datos:

- http://www.ayudaleyprotecciondatos.es/

LOPD y protección de datos (Blog):

- http://proteccion-de-datos-madrid.com/

Blog: Carta de protección de datos

- http://www.cartadeproteccion.com/

IV.DESAYUNE CON MAZARS

TRANSFORMACIÓN Y BUEN GOBIERNO: SU PRINCIPAL COMPETIDOR YA SE ESTÁ PREPARANDO

El compromiso de MAZARS con sus clientes no se detiene en verano. Los próximos meses disminuye la actividad y es un excelente período para el análisis y para que las organizaciones se preparen a posibles cambios. ¿Por qué no **autoevaluarnos** y tratar de **transformar** lo que no nos gusta?

Queremos que conozcas la importancia del papel del **CFO** en los procesos de transformación, que puedes hacer para ser un **catalizador del cambio en tu empresa** y adaptarla de manera rápida y eficiente a los cambios del mercado. Además queremos enseñarte soluciones para **mejorar el buen gobierno, adecuarte a las exigencias regulatorias, y gestionar tus riesgos implantando un modelo de autoevaluación del control interno.**

Para ello te ofrecemos que vengas a desayunar con nosotros y que podamos compartir contigo nuestras experiencias sobre:

- **12 de Junio en Madrid, y 13 de Junio en Barcelona. El CFO aliado del CEO como motor de transformación y del cambio en las organizaciones. Dirigido a Directores Generales y Directores Financieros**.
  Definiremos el papel del CFO en los procesos de transformación, presentaremos los principios para mejorar y simplificar los procesos de tu organización, veremos un caso de éxito y las ventajas que puede aportar el empleo de soluciones tecnológicas.

- **19 de Junio en Madrid y 20 de Junio en Barcelona. Implantación de un Marco de Gestión de Riesgos y de Autoevaluación del Control Interno. Dirigido a Responsables de Control Interno, Auditoría Interna y Cumplimiento Legal**.
  Mostraremos un ejemplo práctico de cómo implantar de una forma efectiva el control interno utilizando como soporte GRIControl©, la herramienta de gestión integral de riesgos de MAZARS, a la que **podrás acceder durante la sesión práctica** si traes tu propio Tablet o Portátil.

Además te daremos la oportunidad de conocer nuestras soluciones en tu empresa, sin grandes inversiones. A los asistentes les ofreceremos la posibilidad de probar estas técnicas en proyectos breves de consultoría, y aprovechar que los empleados vienen más predispuestos al cambio a la vuelta de verano, para comprobar sus resultados.

Evento gratuito con aforo limitado.
Inscríbase en www.mazars.es

V.MÁS INFORMACIÓN, BOLETINES Y EVENTOS MAZARS

MAZARS dispone de especialistas financieros, control interno, auditoría interna, expertos en asesoramiento jurídico, y gestión de riesgos tecnológicos, que participan tanto en proyectos específicos de cada materia, como en equipos multidisciplinares para ofrecer servicios completos de carácter transversal y con garantías que le permitan implantar **soluciones efectivas dentro de los diferentes sectores**.

Si está interesado en que le hagamos una presentación personalizada, por favor no dude en contactar a través de las personas de contacto que aparecen al final del boletín.

Además, puede solicitar que le invitemos a nuestros "**Desayunos Mazars**" de carácter gratuito, así como a nuestro "**Boletín en Auditoría & Control Intern@**" y nuestro "**Boletín LOPD**" enviándonos un e-mail a **auditoria.it@mazars.es**

CONTACTO

MAZARS ***(Más información en www.mazars.es)***
Governance, Risk Management & Compliance

Juan Luque - Socio
+34 934 050 855
juan.luque@mazars.es

Cristina Bausá - Socia
+34 915 624 030
cristina.bausa@mazars.es