Protección de datos

ETL GLOBAL

Índice

1. Presentación

La protección de datos personales es un derecho fundamental reconocido en la Constitución Española que establece la obligación de examinar el empleo que le dan a toda nuestra información.

Cabe resaltar que obliga a empresas y personas que controlen datos de terceros a tratarlos de un modo adecuado y acorde a la legalidad vigente. Ten en cuenta que la ley abarca tanto el marco personal, incluyendo familia y conocidos, como el profesional.

Ante el exceso de manipulación de los datos personales, se ha decidido optar por una nueva forma jurídica que defienda los derechos de todos. Se ha legislado con el objetivo de evitar el mal uso de los datos de los usuarios y para proteger el anonimato de todos ellos.

2. Reglamento

El marco jurídico que trata la Protección de los Datos personales está compuesto por las siguientes normas:

1. Artículo 18.4 Constitución Española
2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
3. 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 diciembre, de protección de datos de carácter personal.
4. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

3. Objetivo del eBook

Conocer a fondo los detalles y anticiparse a la aplicación de la Ley Europea del Reglamento General de Protección de Datos que entrará en vigor el 25 de Mayo de 2018.

Queremos que conozcas las sanciones previstas, los nuevos conceptos y todos los cambios que implica. Al terminar este Ebook estarás preparado para cumplir con esta nueva ley de inminente desarrollo.

mjcriado@etl.es +34 933 942 600 - Mallorca, 272, 3º 08037 Barcelona

4. Nuevo Reglamento Europeo

4.1. Términos y conceptos

A continuación te detallamos todos los conceptos básicos que necesitas conocer del ámbito de aplicación de la Ley de Protección de Datos.

Datos personales

Se considera información personal a todos los datos relativos a una persona física. Esto incluye nombre, apellidos, número de teléfono, dirección postal y dirección de correo electrónico.

Tratamiento

Todas las operaciones sobre datos personales, individuales o colectivos, a través de automatismos o directamente en papel. Esto incluye su uso, la recogida o registro, la conservación y extracción, y cualquier adaptación o consulta realizada sobre ellos.

Elaboración de perfiles

La automatización de los datos personales para elaborar un perfil que nos permita conocer los intereses y el comportamiento, el nivel económico y su localización, y la capacidad profesional y los deseos personales.

Seudonimización

Reducir la unión entre los datos personales y la persona física que los aporta.

Responsable del tratamiento:

Es la persona física o jurídica encargada de defender las garantías que se aplican a los datos personales. Puede ser una autoridad u organismo, una persona física o una persona jurídica.

Encargado del tratamiento o encargado

la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Consentimiento del interesado

Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de sus datos personales.

Datos genéticos

Incluye todos los datos personales de carácter biológico y genético que aporten información exclusiva de una persona. Son aquellos datos obtenidos a través de un análisis que nos ofrezca información sobre la salud y su fisiología.

Datos biométricos

Se incluyen en este punto todos los datos personales relativos al reconocimiento facial y los datos dactiloscópicos de una persona. En definitiva, consiste en toda la información relativa a la conducta y la fisiología de las personas.

4. Nuevo Reglamento Europeo

4.2. Empresas obligadas a cumplir el reglamento

Se aplica a todas las empresas que usen datos personales en el ámbito de la Unión Europea. Ten en cuenta que el reglamento también incluye a los responsables que traten datos conseguidos gracias a los servicios destinados a los ciudadanos de la UE, incluso en el supuesto de que no estén ubicados en los países de la Unión Europea.

4.3 Principios

Licitud, lealtad y transparencia, los datos personales no pueden obtenerse sin el consentimiento del interesado. Es obligatorio que los acepte de una manera lícita. Por eso deberá quedar reflejado el motivo: para ejecutar un contrato, para proteger intereses vitales, para cumplir con un interés público. El responsable debe ofrecer al interesado la información del trato que va a dar a sus datos, siempre de forma clara y de acceso sencillo.

Limitación de la finalidad: los fines deben quedar reflejados sin atisbo de duda y de una manera clara.

Minimización de datos: recoger solo los datos necesarios para el fin o fines marcados. No se pueden pedir otro tipo de datos.

Exactitud y actualización: se deberán adoptar medidas o acciones para corregir los errores en la recogida y la correcta conservación de los datos personales.

Limitación en el plazo de conservación: los datos personales recogidos solo pueden conservarse hasta que se cumpla el fin para el que fueron recolectados. Quedan exentos en este punto los datos recogidos para investigar científicamente o para cumplir con las obligaciones que marca la ley, así como los datos conseguidos por interés público.

Integridad y confidencialidad: es obligatorio tomar las medidas que ayuden a cumplir con ambas.

Responsabilidad proactiva: el nuevo Reglamento sobre protección de datos considera obligatorio usar adecuadamente los datos y obliga al responsable a poder demostrar ante la autoridad que ha actuado correctamente y ha protegido los datos como marca la ley.

4. Nuevo Reglamento Europeo

4.4. Consentimiento expreso y excepciones al mismo

Es vital conocer las novedades que se incluyen en el Reglamento para poder cumplir la ley y evitar multas innecesarias.

1. El responsable tendrá que poder demostrar que obtuvo el consentimiento del interesado para tratar sus datos personales.

2. En ocasiones la solicitud de consentimiento se da por escrito. La declaración debe reflejar claramente y por separado de otros posibles consentimientos, la aceptación del interesado. Deberá diferenciarlo de los otros temas y ofrecer el consentimiento mediante un lenguaje claro, conciso y fácil de entender.

3. La ley defiende los derechos del interesado y le ofrece retirar el consentimiento cuando le parezca necesario. Es obligatorio poner las mismas facilidades tanto para dar como para quitar el consentimiento. La validez del consentimiento anterior a la retirada quedará exento cuando sea revocado por parte del interesado.

Excepciones al consentimiento expreso.

a. Cuando los datos personales son solicitados por un funcionario de una administración pública en el ejercicio de sus funciones.

b. Cuando exista una Ley, que no disponga lo contrario. La Ley 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, señala en su art 8 "que el derecho a la propia imagen, no impedirá la información gráfica sobre un suceso o acaecimiento público, cuando la imagen de una persona determinada aparezca como meramente accesoria".

c. Cuando los datos personales, sean necesarios para el cumplimiento o mantenimiento de un contrato laboral, administrativo. Evidentemente, si nuestros datos personales, se utilizan para un fin distinto de la relación contractual, se requiere del consentimiento.

d. Cuando exista un interés vital del afectado.

e. Que nuestros datos figuren en fuentes accesibles al público.

4. Nuevo Reglamento Europeo

4.5. Derechos de los interesados

La ley protege a todos los ciudadanos con un conjunto de derechos, conocidos como derechos ARCO, que les permite defender su privacidad y el uso que se da a sus datos personales.

ACCESO

Es un derecho imprescindible que permite a los ciudadanos exigir al responsable del fichero la información relativa al uso de los datos y las diferentes comunicaciones realizadas. También sirve para garantizar la transferencia de los mismos en la forma debida.

RECTIFICACIÓN

Es el derecho que defiende al ciudadano para poder modificar los datos personales a través de una solicitud.

CANCELACIÓN

Derecho que ofrece la posibilidad de cancelar y bloquear todos los datos personales. Serán conservados a disposición de Jueces y Administraciones durante el plazo marcado y luego serán suprimidos para siempre.

OPOSICIÓN

Derecho que permite al ciudadano interesado evitar la publicidad de sus datos personales o la comercialización de los mismos. Impide de un modo explicito elaborar perfiles o automatizar su tratamiento.

Este reglamento aporta dos nuevos derechos fundamentales que se unen a los ya mencionados.

OLVIDO O SUPRESIÓN

Es el derecho que te permite cancelar y oponerte al uso de los datos personales en internet.

PORTABILIDAD

Por último, pero no menos importante, se protege el derecho a pedir el traslado de tus datos personales a otra empresa. Podrás pedir al encargado del tratamiento de los datos que te los devuelva de manera automatizada.

Se han protegido todos los derechos del interesado y se ha advertido a los responsables de la obligatoriedad de su correcto cumplimento. Se puede pedir la información electrónicamente y sin cargo para el interesado. Solo en el caso de abusar o pedir datos de manera infundada se podrá cobrar un canon.

4. Nuevo Reglamento Europeo

4.6. Responsable del tratamiento

Se considera responsable del tratamiento a la persona física o jurídica que recopila datos personales de personas para su tratamiento. Tanto si es pública como privada, el responsable deberá llevar a cabo la recopilación de los datos acorde a la legalidad vigente y tomando los medios necesarios para demostrar su correcto cumplimiento.

Escoge el tipo de fichero, así como el objetivo del mismo y el contenido que lo forma. También está obligado a informar y seguir las pautas que marca la legislación o de lo contrario será multado con las sanciones previstas.

Es su responsabilidad escoger a los encargados que puedan acreditar verazmente que se ha cumplido con la ley, adoptando todas las medidas técnicas y de organización que garanticen la seguridad y el buen uso de los datos personales.

4.7. Encargado del tratamiento

Es la persona física o jurídica escogida por el responsable del tratamiento, siempre mediante un contrato de prestación de servicios, para tratar los datos personales de un fichero.

El encargado no puede subcontratar el servicio a un tercero. Solo podría aceptarse este supuesto en el caso de contar con una autorización expresa.

El responsable del tratamiento decide la manera de tratar los datos personales, por lo que el encargado deberá cumplir siempre las instrucciones mandadas.

El nuevo reglamento indica una serie de datos que se deben incluir en el contrato. Deberá quedar reflejada la duración del mismo y el motivo, la naturaleza del tratamiento, los diferentes tipos de datos, las obligaciones, todos los derechos del responsable y por supuesto, la devolución de los mismos al acabar.

4.8. Registro de actividades

El nuevo reglamento suprime la obligación de crear un documento de seguridad y de inscribir los datos en el Registro de la Agencia de Protección de Datos. En su lugar, nos obliga a realizar un **registro de actividades de tratamiento**, siempre que las empresas tengan más de 250 trabajadores, o cuando tengan menos pero el tratamiento pueda entrañar un riesgo para los derechos y libertades o incluya categorías especiales de datos, o incluya datos de condenas e infracciones penales.

El contenido que demanda el registro de actividades es:

- Nombre y datos de contacto del responsable. Si fuera el caso, se debe incluir también el del representante del responsable, el del corresponsable y el del delegado de la protección de los datos personales.
- Fines escogidos para el tratamiento.
- Enumeración de las categorías de datos personales e interesados.
- Todas las transferencias de carácter internacional.
- Si ya se conocen, indicar los plazos para la supresión de los datos personales.
- Describir las medidas de organización y técnicas.

La ley marca la obligatoriedad de que tanto el responsable como el encargado del tratamiento, así como los representantes de los mismos, pongan toda la información a disposición de las autoridades que la soliciten.

En algunas ocasiones, debido a la coincidencia entre los documentos de seguridad y el registro de actividades, podrían usar el primero para llevar a cabo el registro.

4. Nuevo Reglamento Europeo

4.9. Seguridad de los datos personales y comunicación de una violación de seguridad

El reglamento no ofrece un gran número de medidas para la seguridad. Se supone que el responsable y el encargado del tratamiento se encargarán de aplicar la organización y las medidas técnicas necesarias para garantizar la seguridad en base al riesgo. También deberán ser capaces de acceder y disponer de los datos de una manera ágil. Sí que nos da un par de pautas para ayudarnos a cumplir la ley:

a. Recopilar todos los datos que sean necesarios, pero ni uno solo más.

b. Cifrar los datos o seudonimización. Es decir, usar claves secretas o códigos para acceder a los datos y así obligar a consultar información adicional antes de empezar a tratar los datos personales.

El responsable tiene la obligación de notificar a las autoridades cualquier tipo de violación de la seguridad de los datos personales. Deberá hacerlo en menos de 72 horas, salvo que no exista ningún riesgo o requiera de un esfuerzo excesivo.

4.10. Evaluación de impacto

El reglamento puede considerar de alto riesgo el tratamiento de los datos personales. Por eso hay que llevar a cabo una **evaluación de impacto** en los siguientes casos:

- Si se elaboran perfiles que conlleven tomar decisiones que desencadenen efectos jurídicos para los interesados.
- Si se requiere un tratamiento a gran escala de datos de carácter sensible.
- Si se pretende observar una zona de acceso público de amplio espectro.

Al tratase de términos indeterminados, como grandes escalas o amplios espectros, las autoridades requieren que se ofrezca un dato más claro. Para lograrlo se tendrán en cuenta las siguientes valoraciones:

- El número total de interesados que se ven afectados en términos totales, o proporcionalmente a un población concreta.
- Variedad de los datos y volumen total.
- El tiempo que durará la actividad de tratamiento
- Amplitud geográfica de la actividad de tratamiento.

Las autoridades competentes elaborarán un listado de las empresas obligadas a realizar la evaluación de impacto. Se suele tomar como valor el procesamiento de datos a partir de 5000 personas y la evaluación debe incluir obligatoriamente:

- Una descripción clara de la previsión de las operaciones de tratamiento y de los fines de los mismos. Si es menester también se incluirá el interés legítimo que persigue el responsable del tratamiento.
- Una evaluación de la proporcionalidad de las operaciones en base a su finalidad y la necesidad de las mismas.
- Todas las medidas que se han previsto para confrontar los riesgos, incluyendo las garantías y vformas de garantizar la protección de los datos personales acorde al nuevo Reglamento. Se tendrán siempre en consideración los derechos de los interesados y de las personas afectadas.

mjcriado@etl.es +34 933 942 600 - Mallorca, 272, 3º 08037 Barcelona

4. Nuevo Reglamento Europeo

4.11. Consulta previa

Siempre que la evaluación de datos nos demuestre que su tratamiento puede conllevar un alto riesgo y no se haya conseguido identificar o disminuir su influencia, el responsable deberá consultar a la autoridad de control antes de empezar el tratamiento.

2.12. Códigos de conducta

Todas las asociaciones y organismos que representen a las categorías responsables, o a los encargados del tratamiento, pueden elaborar códigos de conducta y modificar los códigos para especificar la aplicación reglamentaria relativa a:

- Un tratamiento transparente y leal
- En contextos muy concretos, los intereses perseguidos por los responsables del tratamiento
- Recopilación de datos personales
- Seudonimización de los datos
- Toda la información ofrecida a los interesados y al público
- Ejercicio de los derechos de los interesados
- Información sobre menores y su protección. Reflejando la forma de conseguir los consentimientos paternos.
- Procedimientos y diferentes medidas
- Notificación a las autoridades y a los interesados de las posibles violaciones de la seguridad de los datos personales.
- Transferencia de los datos a organizaciones internacionales y a otros países.
- Procedimientos extrajudiciales y para solventar conflictos que puedan resolver los diferentes problemas entre los interesados y los responsables.

4.13. Mecanismos de certificación

El nuevo reglamento dicta diferentes fórmulas de certificación para que las empresas puedan acreditar que cumplen con todo lo establecido.

Estas certificaciones del Comité Europeo pueden ser individuales o colectivas y son entregadas por las Autoridades de Protección de Datos o por las entidades colaboradoras acreditadas.

4. Nuevo Reglamento Europeo

4.14. Delegado de protección de datos

El reglamento ha creado la figura del Delegado de Protección de Datos para que vele, conjuntamente con el Responsable y el Encargado del tratamiento, por el correcto cumplimiento de la normativa para las empresas en los siguientes casos:

- Si lo lleva a cabo un organismo público o una autoridad competente
- Si es tan masiva que necesita una observación continua y sistemática o si hace referencia a los interesados a gran escala.
- Con objetivos sobre condenas o infracciones de carácter penal o por categorías especiales de datos personales.

Las funciones destacadas del Delegado de Protección de Datos son:

- Proporcionar información y asesoría, así como supervisar a los trabajadores, responsables y encargados relativos al cumplimiento la protección de datos personales.
- En el supuesto que sea necesario, asesorar sobre la evaluación de impacto.
- Colaborar siempre con la autoridad de control

El Delegado de Protección de Datos puede ser un profesional externo contratado por un servicio, trabajador de una Administración Pública o formar parte de la plantilla de la empresa.

Eso sí, en todos los casos se pide la total garantía de independencia sobre los directivos y que se pongan a su disposición todos los medios para poder desempeñar su trabajo.

4.15. Transferencias internacionales

Hace referencia a la comunicación de los datos personales a personas ajenas a la empresa fuera del país de origen, haciendo hincapié en los países que no ofrecen las mismas garantías reflejadas en el nuevo Reglamento sobre la protección de datos personales.

La legislación vigente garantiza que los datos tratados por la empresa se usarán en el extranjero con los mismos derechos que tienen en su país de origen.

Debido a que el Reglamento tiene vigencia en la Comunidad Económica Europea, no necesita autorización de la Agencia de Protección de Datos para países de la unión.

También se ha llegado a un acuerdo con los Estados Unidos, por lo que la transferencia de datos personales entre este país y Europa se realizará manteniendo siempre unos principios básicos acordados por ambas partes.
El acuerdo incluye el denominado Privacy Shield para las transferencias entre américa y Europa. De esta manera se podrán hacer las transferencias de datos sin tener que pedir autorización a la Agencia de Protección de Datos. La empresa norteamericana deberá estar adherida al Privacy Shield y tendrá que informar a la agencia de todos los movimientos.

Si se deben transferir datos personales a otros países será obligatorio pedir la autorización a la Agencia de Protección de Datos.

4.16. Sanciones

Ten siempre presente que han aumentado las sanciones dispuestas para el nuevo Reglamento. Se ha establecido que las multas pueden llegar a los 20 millones de euros o al cuatro por ciento del volumen de negocio de la empresa infractora.

También han decidido tener en cuenta a la hora de multar la efectividad del daño creado, si se ha colaborado con las autoridades competentes o si se ha respetado el principio de proporcionalidad. Presta especial atención para operar siempre dentro de la legalidad vigente.

5. Conclusión

La nueva legalidad, que entrará en vigor el próximo mes de mayo, ofrece a las empresas una mayor independencia para organizar y proteger los datos personales. A cambio nos demanda mucha más atención y rigor para poder demostrar que la empresa ha actuado de forma correcta.

Para terminar, te recuerdo que está prohibido y penado recoger datos personales sin el consentimiento de los titulares.

mjcriado@etl.es +34 933 942 600 - Mallorca, 272, 3º 08037 Barcelona

www.etlglobalnexum.com

Carrer de Mallorca, 272 3ª planta
08037 Barcelona
Barcelona
+34 933 942 600

¡Síguenos en nuestras Redes Sociales!

Protección de datos

ETL® GLOBAL