C. Mallorca 260
08008 Barcelona
Tel. 932 155 989
www.auren.com

auren

CERCA DE TI PARA LLEGAR LEJOS

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Enfoque práctico

Albert Lladó Palau
Socio director del área de Gobierno, Riesgos y Cumplimiento de Auren
albert.lladó@bcn.auren.es

Barcelona, 5 de julio de 2018

auren

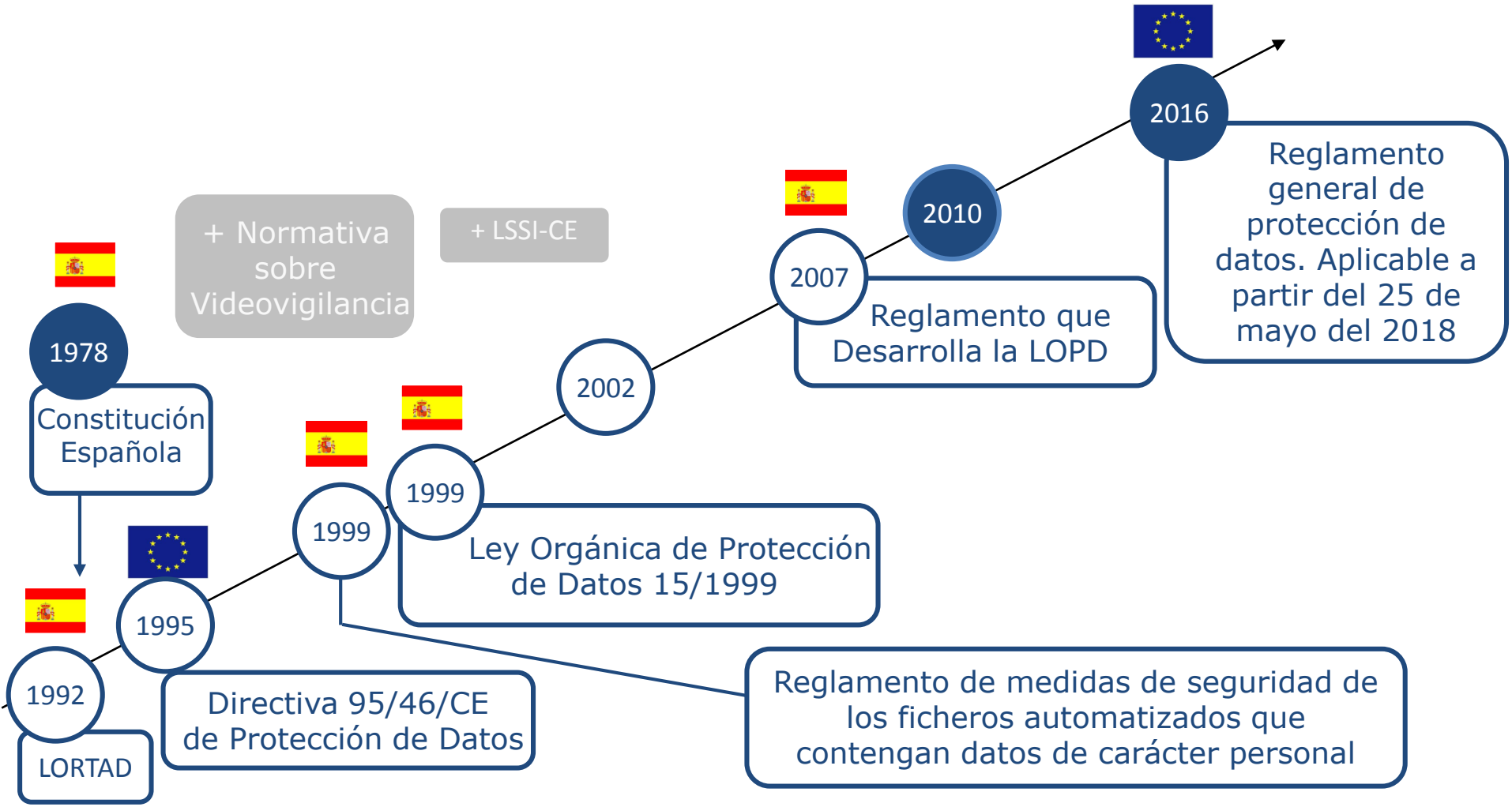
MEMBER OF THE FORUM OF FIRMS

Índice

- Introducción al reglamento
- Novedades del nuevo reglamento general
- Nuevas obligaciones
- Infracciones y sanciones
- Implicaciones prácticas

INTRODUCCIÓN AL REGLAMENTO

INTRODUCCIÓN AL REGLAMENTO



¿POR QUÉ DEBO PROTEGER LOS DATOS DE CARÁCTER PERSONAL?

- El artículo 12 de la **Declaración Universal de Derechos Humanos** establece lo siguiente:

> *"Nadie será objeto de ingerencias arbitrarias en su **vida privada**, **su familia**, **su domicilio o su correspondencia, ni de ataques a su honra o reputación**. Toda persona tiene derecho a la protección de la ley contra tales ingerencias o ataques".*

- El **Reglamento UE 2016/679 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, establece:

> *"El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su **derecho a la protección de los datos personales"**.*

POR QUÉ DEBO PROTEGER LOS DATOS DE CARÁCTER PERSONAL?

- La **Constitución española** reconoce en sus **Derechos Fundamentales**, en concreto en los arts. 16.2 y 18:
  - **Intimidad**
  - **Honor**
  - **Propia imagen**

*Derecho fundamental que garantiza a toda persona un **poder de control** sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado.*

INTRODUCCIÓN AL REGLAMENTO

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)

Evolución tecnológica y globalización → Respuesta a nuevos retos no regulados

Diferentes niveles de protección entre los estados → Armonizar normativa

INTRODUCCIÓN AL REGLAMENTO

Ámbito de aplicación material

Se aplica: a **tratamientos automatizados, semiautomatizados o no automatizados**, de datos personales incluidos o destinados a ser incluidos en ficheros.

No se aplica a tratamientos de datos personales en el ejercicio de actividades:

- no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.
- llevadas a cabo por parte de los Estados miembros en el ámbito de política exterior y de seguridad común.
- exclusivamente personales o domésticas.
- llevadas a cabo por autoridades competentes con finalidades de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales.

Ámbito de aplicación territorial

Se aplica a tratamientos de datos personales:

- llevados a cabo por un responsable o encargado cuyo **establecimiento** esté **ubicado en la Unión** (independientemente de que el tratamiento tenga lugar en la Unión o no).
- **de interesados que residen en la Unión**, por parte de un responsable o encargado no establecido en la Unión, cuando:
  - Oferta de bienes o servicios a interesados de la Unión.
  - Control del comportamiento que tenga lugar en la Unión.
- por parte de un responsable que no esté establecido en la Unión, pero al que el Derecho de la Unión le es aplicable, en virtud del Derecho Internacional Público.

INTRODUCCIÓN AL REGLAMENTO

PRINCIPIO DE
LICITUD, LEALTAD Y TRANSPARENCIA
Los datos personales serán tratados de forma lícita, leal i transparente en relación al interesado.

PRINCIPIO DE
LIMITACIÓN DE LA FINALIDAD
Fines determinados, explícitos y legítimos.
No tratar los datos de forma incompatible con los fines.
No se considera incompatible el tratamiento con fines de archivo en interés público, de investigación científica o histórica, o estadísticos.

PRINCIPIO DE
MINIMIZACIÓN DE DATOS
Datos adecuados, pertinentes y limitados a lo que sea necesario.

PRINCIPIO DE
EXACTITUD
Exactos y puestos al día.

PRINCIPIO DE
LIMITACIÓN DEL PLAZO DE CONSERVACIÓN
No más tiempo del necesario para los fines del tratamiento.
Podrán conservarse por más tiempo con fines de archivo en interés público, de investigación científica o histórica, o estadísticos.

PRINCIPIO DE
INTEGRIDAD Y CONFIDENCIALIDAD
Tratamiento que garantice la integridad y confidencialidad de los datos.

RESPONSABILIDAD PROACTIVA
El responsable del tratamiento será responsable del cumplimiento de los principios anteriores y deberá de ser capaz de demostrarlo.


NOVEDADES DEL
NUEVO
REGLAMENTO
GENERAL

¿Qué es un dato personal?

LOPD

Dato de carácter personal:

Cualquier información referida a personas físicas identificadas o identificables.

REGLAMENTO UE

Datos personales:

Toda información sobre una persona física identificada o identificable.

Que se pueda determinar su identidad, directa o indirectamente, a partir de:

Nombre, número de identificación, datos de localización, identificador en línea, elementos propios de identidad física, fisiológica, genética, psíquica, económica, cultural, o social.

Categorías especiales de datos personales

Ideología

Afiliación sindical

Religión

Creencias

Origen racial

Salud

Vida sexual

Orientación sexual

Datos genéticos

Datos biométricos

Información

Se tendrá que informar al interesado en el momento en que se obtengan los datos personales sobre:

De forma concisa, transparente, inteligible y de fácil acceso, en un lenguaje claro y sencillo

- La **existencia** de un fichero, la **finalidad** del mismo y de los **destinatarios** de la información
- Del **carácter obligatorio o facultativo** de la respuesta
- **Consecuencias** de la obtención de los datos y de la negativa de suministrarlos
- Posibilidad de **ejercer los derechos ARCO**
- Identidad y **dirección del responsable del fichero** y, en su caso, del representante
- Datos de contacto del **delegado de protección de datos,** en su caso
- **Base jurídica** del tratamiento (*consentimiento, relación contractual, intereses vitales del interesado, obligación legal…)*
- **Intereses legítimos** del responsable o de terceros, en su caso
- Intención de **transferir los datos a un tercer país** o a una organización internacional y la base para hacerlo, en su caso
- **Plazo durante el cual se conservarán los datos**
- Derecho a solicitar la **portabilidad y la limitación del tratamiento** de los datos.
- Derecho a **retirar en cualquier momento el consentimiento** que se haya prestado, en su caso
- Si la **comunicación de datos** es un requisito legal o contractual o un requisito necesario para suscribir un contrato
- Derecho a presentar una **reclamación ante una autoridad de control**
- **Existencia de decisiones automatizadas, incluida la lógica aplicada y sus consecuencias**

Derechos de los interesados

El derecho a la portabilidad es una forma avanzada de derecho de acceso

Derecho a obtener una copia de los datos personales tratados

Consecuencia del cual es el derecho al olvido

Derechos de los interesados

Derecho al olvido

- **¿Cuándo se puede ejercer?**
  - Datos no necesarios
  - Revocación consentimiento
  - Oposición al tratamiento
  - Tratamiento ilícito
  - Menores
  - Supresión basada en obligación legal
- **Excepciones**
  - Libertad de expresión e información
  - Obligación legal
  - Finalidades científicas, históricas, estadísticas o interés público
  - Reclamaciones
  - Limitación del tratamiento

Derecho a la limitación del tratamiento

Supone que, a petición de la persona interesada, no se aplicarán a sus datos las operaciones de tratamiento que en cada caso corresponderían.

- **¿Cuándo se puede ejercer?**
  - Interesado solicita la rectificación u oposición y mientras el responsable determina si procede atender la solicitud.
  - Tratamiento ilícito o datos no necesarios y hay que borrarlos, pero el interesado se opone a ello.
- **Excepciones**
  - Consentimiento del interesado
  - Reclamaciones
  - Protección de los derechos de otra persona
  - Interés público

Derecho a la portabilidad

Permite al interesado recibir los datos personales que le afectan y que ha facilitado a un responsable de tratamiento o solicitar que sean transmitidos directamente a otro responsable de tratamiento

- **¿Cuándo se puede ejercer?**
  - Tratamientos automatizados basados en el consentimiento o en un contrato
  - Sólo de sus datos (no de terceros) y que haya proporcionado él o derivados de su actividad

Consentimiento

Se exige una <u>manifestación de voluntad</u>:

Inequívoca (no hay posibilidad de error)

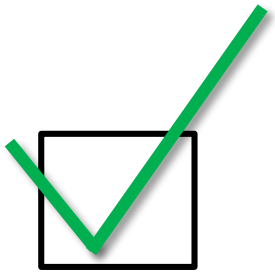
Libre (no forzada)

Específica (finalidad concreta-finalista)

Informada (hay que comunicar previamente la información)

Expresa ~~o tácita~~ (explícita)

Acto afirmativo (no es válida la inacción)



<u>Consentimiento del niño</u>
Mayor de 16 años
*Los Estados Miembros podrán rebajar la edad hasta el mínimo de 13 años.

<u>Revocación del consentimiento</u>
Siempre es posible.
Sin carácter retroactivo.

NOVEDADES DEL NUEVO REGLAMENTO GENERAL

Códigos de conducta y mecanismos de certificación

Códigos de conducta

Se promueve la creación de códigos de conducta, **que habrá que presentar a la autoridad de control para que los apruebe, registre y publique**. La **supervisión** del cumplimiento del código la realizará un **organismo acreditado** por la autoridad de control competente.

La adhesión a un código tipo sirve para **demostrar que se está cumpliendo la normativa** y se tendrá en cuenta a la hora de sancionar.

Mecanismos de certificación, sellos y marcas

Como en el caso de los códigos de conducta, su objetivo es **demostrar el cumplimiento de la normativa** y se tendrá en cuenta a la hora de sancionar.

La certificación la tiene que **expedir un organismo de certificación acreditado** o bien la **autoridad de control** y será **válida por 3 años**.

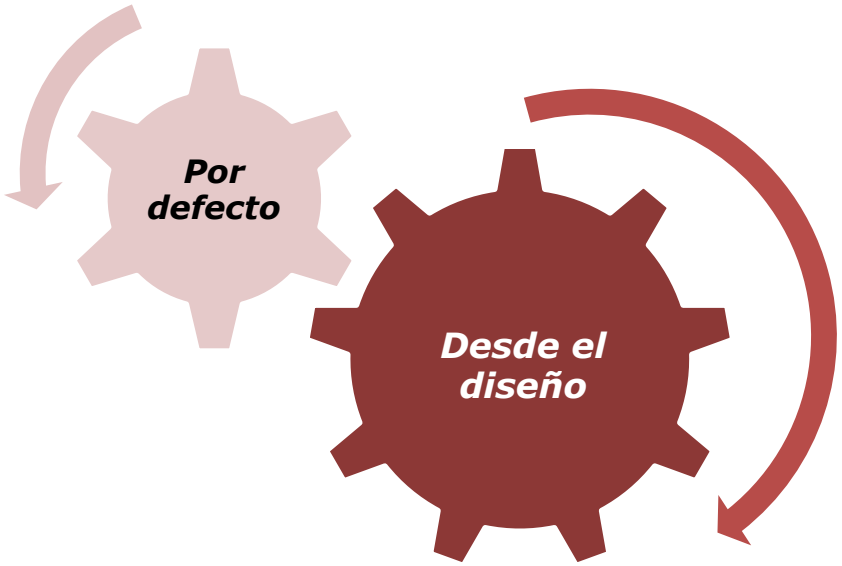
Los organismos de certificación son los responsables de la correcta evaluación de la certificación y de su retirada, en su caso. Serán acreditados por la autoridad competente o por el organismo nacional de acreditación que corresponda (ENAC). Su acreditación será válida durante 5 años.


NUEVAS
OBLIGACIONES

Protección de datos desde el diseño y por defecto

Garantizar que, **por defecto**, sólo sean objeto de tratamiento los **datos personales que sean necesarios**.

- Extensión del tratamiento
- Plazo de conservación
- Accesibilidad



Obligación de aplicar medidas técnicas y organizativas para proteger los derechos de los interesados, tanto en el **momento de determinar los medios del tratamiento** como en el momento del propio tratamiento.

- Seudonimización
- Minimización de datos
- Garantías necesarias

Registro de las actividades del tratamiento

Supuestos

a. Empresas con más de **250 trabajadores**.
b. Empresas que realicen tratamientos que puedan **comportar un riesgo para los derechos y libertades de los interesados**.
c. Tratamientos no ocasionales.
d. Empresas que incluyan **categorías especiales** de datos personales o datos personales relativos a **condenas e infracciones penales**.

Contenido

1. Nombre y datos de **contacto del responsable y del delegado** de protección de datos.
2. **Finalidades** del tratamiento.
3. Descripción de las **categorías de interesados** i de las **categorías de datos personales.**
4. **Categorías de destinatarios.**
5. **Transferencias internacionales** y las garantías aplicadas.
6. **Plazos previstos.**
7. Descripción general de las **medidas de seguridad**.

- El registro estará **a disposición de la autoridad de control**.

Evaluación de impacto

Supuestos

a) **Tratamientos automatizados** sobre los que se tomen decisiones que produzcan efectos jurídicos para personas físicas (p.e. Elaboración de perfiles).
b) **Tratamiento a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones penales.**
c) Observación sistemática a gran escala de una **zona de acceso público** (p.e. Videovigilancia).

La autoridad de control publicará una lista con las operaciones que requieran una evaluación de impacto.

Contenido de la evaluación

1) Descripción de las operaciones y los fines que se persiguen.
2) Interés legítimo del responsable.
3) Necesidad y proporcionalidad de las operaciones respecto a la finalidad.
4) Evaluación de los riesgos.
5) Medidas previstas.

Documentado

- *Se debe realizar con el asesoramiento del Delegado de protección de datos.*
- *Obligación de consulta a la autoridad de control si de la evaluación de impacto resulta que el tratamiento previsto puede infringir el RGPD, en particular cuando el responsable no ha identificado o mitigado suficientemente el riesgo.*

Medidas de seguridad

El nuevo reglamento general no regula específicamente las medidas de seguridad que se tendrán que aplicar, sino que se limita a indicar que habrá que aplicar las medidas técnicas y organizativas adecuadas al riesgo que comporte el tratamiento, entre otras:

- ✓ Seudonimización y cifrado.
- ✓ Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- ✓ Capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente físico o técnico.
- ✓ Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas.

Encargos de tratamiento

Se amplían los extremos que debe contener el contrato:

- ✓ el objeto y la duración del encargo
- ✓ la naturaleza del tratamiento
- ✓ el tipo de datos personales
- ✓ las categorías de interesados
- ✓ las obligaciones y los derechos del responsable
- ✓ la previsión de que las personas que van a tratar los datos se comprometan a mantener la confidencialidad
- ✓ la asistencia del encargado al responsable para atender las solicitudes de ejercicio de derechos
- ✓ la supresión o la devolución de los datos al finalizar el encargo
- ✓ la obligación de poner a disposición del responsable toda la información necesaria para demostrar que cumple las obligaciones del encargado del tratamiento y para permitir y contribuir a que el responsable u otro auditor autorizado por el responsable efectúe auditorías e inspecciones

Se les **atribuyen determinadas obligaciones**: mantener un registro de actividades de tratamiento, determinar las medidas de seguridad aplicables, designar a un DPD…

Se establece la **obligación de diligencia debida en la selección de encargados**. Los responsables sólo deben escoger encargados que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.

NUEVAS OBLIGACIONES

Notificación de las violaciones de seguridad

	Notificación a la autoridad de control	Comunicación al interesado
Plazo	72 horas desde que se tiene constancia Si +72 horas → motivos de la dilación	Sin dilación indebida

Transferencias internacionales

Delegado de Protección de Datos (DPD)

Diferencias con el responsable de seguridad

Responsable de seguridad

- **Ficheros de nivel medio o alto**
- **Persona física de la organización**

Delegado de protección de datos

- **Autoridad u organismo público**
- **Observación habitual y sistemática de interesados a gran escala** *(p.ej. hospitales, empresas de seguros, bancos, proveedores de telefonía...)*
- **Categorías especiales de datos y datos relativos a condenas e infracciones penales.**

En el resto de supuestos: "se podrá"

- Parte de la plantilla o contrato de servicios
- Un grupo empresarial, o una autoridad u organismo público, podrán designar a un único delegado de protección, teniendo en cuenta su estructura organizativa.
- Será designado atendiendo a sus cualidades profesionales.


INFRACCIONES
Y SANCIONES

INFRACCIONES Y SANCIONES

Toda persona que haya sufrido daños y perjuicios, materiales o inmateriales, como consecuencia de una infracción del Reglamento, tendrá derecho a recibir, del responsable o del encargado de tratamiento, una **indemnización**.

Únicamente responderá:

a) cuando no haya cumplido las obligaciones dirigidas específicamente a los encargados.

b) cuando haya actuado al margen de las instrucciones legales del responsable.

Cuando participe más de un responsable o encargado, cada uno de ellos será considerado responsable de todos los daños y perjuicios.

INFRACCIONES Y SANCIONES

Máximo **10.000.000 €** o **2%** **del volumen de negocio total anual global** del ejercicio financiero anterior en caso de empresas	1) Obligaciones del **responsable** y del **encargado** en referencia a: • Consentimiento del niño. • Tratamiento que no requiere identificación. • Funciones del delegado de protección de datos. • Certificaciones. • ... 2) Obligaciones de los **organismos de certificación**. 3) Obligaciones de la **autoridad de control** en referencia a la supervisión de los códigos de conducta aprobados.
Máximo **20.000.000 €** o **4%** **del volumen de negocio total anual global** del ejercicio financiero anterior en caso de empresas	1) Principios básicos del tratamiento en referencia a: • Principios relativos al tratamiento. • Licitud del tratamiento. • Condiciones para el consentimiento. • Tratamiento de categorías especiales de datos. 2) Derechos de los interesados. 3) Transferencias internacionales. 4) Obligaciones que adopten los estados miembros en materia de: • Tratamiento y libertad de expresión e información. • Tratamiento y acceso del público a documentos oficiales. • Tratamiento del número nacional de identificación. • Tratamiento en el ámbito laboral. • Tratamiento con finalidades de archivo en interés público, de investigación científica o histórica o estadísticas. • Obligaciones de secreto. • Tratamiento de datos de la Iglesia y asociaciones religiosas. 5) Incumplimiento de una resolución o limitación, temporal o definitiva, del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control. 6) No facilitar acceso a la autoridad de control para llevar a cabo una investigación.

IMPLICACIONES PRÁCTICAS

IMPLICACIONES PRÁCTICAS

Ejemplos de riesgos asociados a la protección de datos:

- Pérdidas económicas por incumplimiento de la legislación.
- Pérdida de competitividad del producto o servicio, o de clientes, derivada de daños reputacionales o causados por carencia de medidas de seguridad adecuadas.
- Obtener consentimiento dudoso/inválido para el tratamiento de datos.
- En entornos web, ubicar la información sobre protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización.
- Inexistencia de contrato adecuado con los encargados de Tratamiento.
- Carencia de procedimientos para la gestión de los derechos ARCO.

IMPLICACIONES PRÁCTICAS

- No se trata de algo que se pueda escoger, **<u>TODAS</u> las empresas que tratan datos de carácter personal están obligadas a ello.**
- **El coste de adaptación es bajo, el coste de <u>NO</u> adaptación es altísimo.**
- La fusión entre los servicios legales, cumplimiento e informáticos garantiza una buena implantación profesional, ya que es un **ámbito multidisciplinar con componentes legales, organizativos y técnicos** con un coste de adaptación global razonable.

Actividades para la adecuación al reglamento general

- ✓ **Registro documental de actividades**
- ✓ **Evaluación de impacto**
- ✓ **Adecuar las medidas de seguridad**
- ✓ **Plan de acciones a realizar**
  - Sistema de notificación de incidencias
  - DPD
  - Revisión de les cláusulas de información, de los mecanismos de obtención del consentimiento, de los contratos de encargado de tratamiento, de los mecanismos para realizar transferencias internacionales...
- ✓ **Formación y concienciación**
- ✓ **Mejora continua**
- ✓ **Revisión periódica**

Gracias por su atención

¿Ruegos y preguntas?

auren

CERCA DE TI PARA LLEGAR LEJOS

AUREN ESPAÑA

www.auren.es

A Coruña - Alicante - Barcelona - Bilbao - Cartagena - Las Palmas de Gran Canaria
Madrid - Málaga - Murcia - Palma - Sevilla - Valencia - Valladolid - Vigo - Zaragoza

AUREN INTERNACIONAL

www.auren.com

Alemania - Argentina - Chile - Colombia - Países Bajos - México - Portugal – Uruguay

PRESENCIA EN OTROS LUGARES DEL MUNDO:

Miembro de:

Antea
ALLIANCE OF INDEPENDENT FIRMS

www.antea-int.com