PRINCIPALES NOVEDADES DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS. ASPECTOS JURÍDICOS

auda

CONSULTORES LOPD y LSSI

ÍNDICE

auda
CONSULTORES LOPD y LSSI

1. COEXISTENCIA DE NORMAS REGULADORAS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal **[LOPD]**
- 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 **[RDLOPD]**

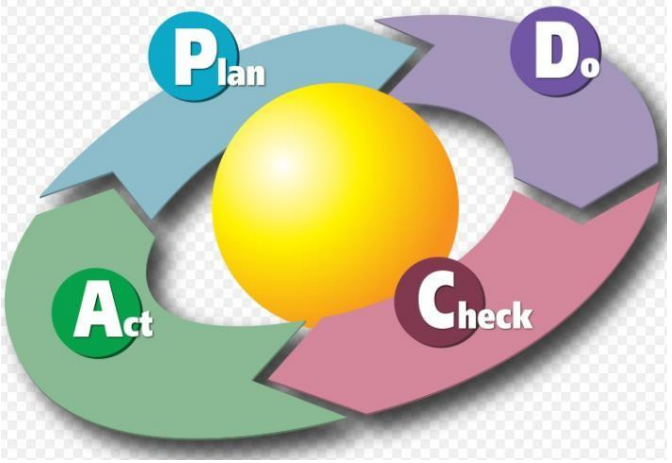
- Directiva 95/46/CE del Parlamento europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos **[Directiva 95/46/CE]**.
- Reglamento (UE) 2016/679 del Parlamento Europeo 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 **[RGPD]**.

2. ¿CUÁL ES SU OBJETO Y CUÁNDO SERÁ EXIGIBLE EL RGPD?

- Es un intento de **armonizar u homogeneizar la normativa europea sobre protección de datos.**
- Entró en vigor el 24 de mayo de 2016. Norma de efecto directo que **no requiere trasposición al derecho interno,** a diferencia de una Directiva.
- Será **aplicable a partir del 25 de mayo de 2018** (Artículo 99 RGPD), de modo que hasta la fecha deberemos realizar una **adaptación progresiva.** Debemos ir preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones del RGPD.

auaa
CONSULTORES LOPD y LSSI

- Por tanto **todas las empresas** deberían estar YA adecuados a la LOPD, así como:
  - Mantener actualizado su documento de seguridad.
  - Realizar los correspondientes controles periódicos.
  - Y realizar las auditorias con la periodicidad bienal exigida por el RDLOPD.



- Y progresivamente deberán adecuarse al RGPD antes del 25 2018.

3. ¿CUÁLES SON LAS PRINCIPALES OBLIGACIONES?

(a) Notificación e inscripción de ficheros al RGPD.

(e) Deber de información del interesado y, en su caso, la **obtención del consentimiento** para el tratamiento de su información de carácter personal.

(i) Formalización de **contratos de acceso a datos por cuenta de terceros** y contratos de **prestación de servicios sin acceso a datos**.

(o) Elaboración del Documento de seguridad e implantación de medidas de seguridad de carácter técnico y organizativo en el sistema de información.

(u) Información, concienciación o sensibilización del personal: Usuarios y Responsables de Seguridad.

****Derechos** Acceso, Rectificación, Cancelación, Oposición (A.R.C.O.)

** **Auditoria** anual, de las medidas de seguridad.

(a) Registro de Actividades de Tratamiento de datos personales

(e) Deber de informar y **(i)** Acuerdos o contratos de encargo de tratamiento.

(o) Responsabilidad proactiva:
- Notificación violaciones de seguridad (interesado o autoridad de control
- Privacidad desde el diseño y por defecto
- Evaluaciones de Impacto en la Privacidad (EIPD)
- Accontability

(u) Delegado de Protección de Datos (DPO)

** **ARCO +** Derecho portabilidad y Derecho de supresión (olvido)

** Auditoria *sine díe*. Sometimiento a control y verificación

3.1.-El Registro de Actividades de Tratamiento

NO notificación a la autoridad de control.

NOTIFICACIONES TELEMATICAS A LA AEPD

Inscripción de Ficheros

Nombre del fichero: AGENDA CONTACTOS TERCEROS
Finalidad: CONTIENE DATOS DE CONTACTO DE TERCEROS EN GENERAL NECESARIOS PARA EL MANTIEMIENTO DE LA RELACION CON LOS MISMOS

Nombre del fichero: CONTABILIDAD
Finalidad: PERMITE LA GESTION DE LA CONTABILIDAD DE LA EMPRESA COBROS Y PAGOS FISCAL Y DE FACTURACION

Nombre del fichero: CURRICULUMS
Finalidad: GESTION DE SELECCION Y PROMOCION DE PERSONAL

Nombre del fichero: EXPEDIENTES
Finalidad: CONTIENE LOS DATOS RELATIVOS A LOS EXPEDIENTES JUDICIALES Y EXTRAJUDICIALES PERMITE LA GESTION CONTABLE FISCAL Y ADMINISTRATIVA DE LOS CLIENTES LA LLEVANZA DE LOS ASUNTOS EL CONTROL DE COBROS Y PAGOS PERMITE LA FIDELIZACION DE LOS CLIENTES Y EN GENERAL EL MANTENIMIENTO DE LA RELACION ABOGADO/ASESOR CON EL CLIENTE

Nombre del fichero: PROVEEDORES
Finalidad: CONTIENE DATOS IDENTIFICATIVOS Y DE CONTACTO DE PROVEEDORES CON EL FIN DE MANTENER LA RELACION MERCANTIL CON LOS MISMOS

Registro a nivel interno y «a disposición de la autoridad de control que lo solicite».

3.1.1. El tratamiento como protagonista….

- **El RGPD desplaza el centro de gravedad desde los ficheros hacia los tratamientos**

Fichero ➡ Tratamiento

Dato Personal ➡ uso que se realiza del Dato Personal (para qué y cómo se utiliza).

Definiciones (art 4 RGPD)

Art. 4.2: Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Art. 4.6: Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

¿Y los anteriores ficheros físicos que relacionábamos en el Documento de Seguridad….?

3.2 Tipología de datos . Las categorías especiales de datos (art 9 y 10 RGPD)

Datos sensibles o especialmente protegidos

- ❑ Opiniones políticas, Ideología
- ❑ Convicciones religiosas o filosóficas, Creencias
- ❑ Afiliación sindical
- ❑ Origen étnico o racial
- ❑ Datos relativos a la salud (física o psíquica)
- ❑ Víctimas de violencia de género
- ❑ Vida sexual

+

Categorías especiales de datos

- ❑ Orientación sexual
- ❑ Datos genéticos
- ❑ Datos biométricos
- ❑ Condenas e infracciones penales o medidas de seguridad relacionadas

auda
CONSULTORES LOPD y LSSI

3.3. El Registro de actividades del tratamiento

- El registro de las actividades de tratamiento sustituye al documento de seguridad actual.
- Sigue siendo un documento interno «a disposición de la autoridad de control que lo solicite».
- Sujetos obligados: el responsable y el encargado (el suyo propio y respecto a las categorías de actividades de tratamiento efectuadas por cuenta del responsable).
- Excepción (30.5 RGPDUE): No resulta obligatorio para empresas u organizaciones que empleen a menos de 250 trabajadores, salvo:
  - ✓ Riesgo para los derechos y libertades de los interesados.
  - ✓ No ocasional.
  - ✓ Incluya categorías especiales de datos o de condenas e infracciones penales.
- Registro «constará por escrito, inclusive en formato electrónico».
- Contenido: art 30 RGPDUE.

auda
CONSULTORES LOPD y LSSI

Recomendación ¿Cómo articular el Registro de Actividades de Tratamiento? [Vid. *Guía del RGPD para Responsables de Tratamiento*]

1º Partir de los ficheros que actualmente tienen inscritos en el Registro General de Protección de Datos (**RGPD**),

2º Desgajar las operaciones de tratamiento concretas vinculándose a una finalidad básica común de todas ellas (por ejemplo, "gestión de clientes", "gestión contable" o "gestión de recursos humanos y nóminas") o con arreglo a otros criterios distintos.

EJEMPLO

Fichero "Trabajadores"

Tipificación de finalidades o usos de los datos:

- Recursos Humanos [Gestión; Formación; Selección; Promoción; Control horario]
- Gestión de Nóminas
- Prevención de riesgos laborales

Tratamientos asociados

1. Tratamiento Contratación empleados
2. Tratamiento Gestión de Nóminas
3. Tratamiento Control horario

auda
CONSULTORES LOPD y LSSI

3.2. EL deber de información [Artículo 13 y 14 RGPD] (Clausulado informativo)

- Además de la información establecida por la LOPD, se han de añadir otros extremos:
  - Datos de contacto del Delegado de Protección de Datos.
  - La base jurídica o legitimación para el tratamiento (consentimiento, ejecución de un contrato; cumplimiento de una obligación legal; misión en interés público o ejercicio de Poderes públicos; interés legítimo del Responsable o un tercero)
  - Informar de las transferencias internacionales de datos.
  - Plazo s o criterios de conservación de los datos.
  - Derecho reclamación ante una autoridad de control.
- Y, adicionalmente, en el caso de que los datos no se obtengan del propio interesado
  - El origen o procedencia de los datos
  - Las categorías o tipos de datos (identificativos, características personales, etc.)

auda
CONSULTORES LOPD y LSSI

¿ Cómo ha de ser la información? [Vid. *Guía para el cumplimiento del deber de informar*]

- Deberá proporcionarse la información **de forma concisa, transparente, inteligible y de fácil acceso**.
- Con un **lenguaje claro y sencillo, comprensible**: Evitar las fórmulas especialmente farragosas. Se debe buscar un equilibrio entre concisión y precisión, evitando circunloquios, explicaciones innecesarias o detalles confusos. Evitar el abuso de citas legales, "jerga" confusa, o términos ambiguos o con escaso sentido para las personas destinatarias.

¿ Cuándo han de estar listas las cláusulas conforme al RGPD?

- **Cuanto antes.** Puesto que los nuevos requisitos amplían y no contradicen la obligación de informar establecida en la LOPD, se recomienda revisar y aplicar dicha adaptación cuanto antes
- **Los procedimientos, modelos o formularios diseñados de conformidad con la LOPD deberán ser revisados y adaptados con anterioridad a la fecha** de plena aplicación del RGPD, incorporando los nuevos requisitos de acuerdo con las directrices transmitidas por las autoridades de control.

auda
CONSULTORES LOPD y LSSI

Cuestiones importantes relativas al deber de información.

❑ ¿Quién y cuándo debe informar?

- ✓ La obligación recae sobre el Responsable del Tratamiento.
- ✓ La información se debe proporcionar en el momento en que se soliciten los datos, previa recogida o registro de los mismos, si se obtienen directamente del interesado.
- ✓ Si los datos no se obtienen directamente del interesado (cesión legítima / fuentes accesibles al público):
  - Antes de un mes desde que se obtuvieron los datos
  - Antes o en la primera comunicación con el interesado.

❑Las autoridades de Protección de Datos recomiendan adoptar un modelo de información por capas o niveles

El enfoque de la información multinivel consiste en lo siguiente:

- ✓ Presentar una información básica en un primer nivel, de forma resumida en el mismo momento y en el medio en que se recogen los datos,
- ✓ Remitir la información adicional en un segundo nivel donde se presentarán detalladamente el resto de informaciones en un medio más adecuado para su presentación, comprensión y si se desea, archivo.

auda
CONSULTORES LOPD y LSSI

Información por capas [Vid. *Guía para el cumplimiento del deber de informar*] .

Modelo orientativo.

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

¿ Cómo y dónde articular la información? Información por capas

Información básica (1ª capa)	Información adicional (2ª capa)
Dónde ha de recogerse	
Debería situarse en el mismo **"campo de visión"** , según sea el medio utilizado en la recogida de los datos	Depende de las características del medio empleado para informar, si bien ya no debe estar condicionada en cuanto a la extensión de la información. Las posibilidades, en este caso, son más flexibles.
En papel	
Debería situarse en el mismos lugar donde están los campos a cumplimentar. Si, por restricciones del diseño, no fuese factible, debe incorporarse una nota o llamada en el campo de visión de la firma, informando sobre dónde se sitúa la tabla con la información sobre protección de datos. Ejemplo: "*antes de firmar la solicitud, debe leer la información básica sobre protección de datos que se presenta en (…el reverso, al pié, etc…)*"	▪ En el mismo formulario cumplimentado (por ejemplo, en el **reverso)** ▪ Como un **anexo** o separata que se entregue al interesado y que pueda conservar ▪ Como información expuesta, claramente visible, en **carteles**, paneles, trípticos, etc, de los cuales se pueda solicitar una **copia manejable para conservar**.
Medios electrónicos	
Debería situarse donde está el **botón de "Enviar".** Es recomendable que, para información adicional o complementaria, se incluya en hipervínculo a la misma. Ejemplo: + info	▪ En una página web específica, a la que se accede mediante un hipervínculo ▪ Como un documento disponible para su descarga desde una URL ▪ Como información anexa o adjunta a un mensaje electrónico dirigido al interesado
Telefónicamente	
Como una ***locución clara y concisa, pero asegurando que el interlocutor haya comprendido la información*** suministrada, antes de proceder a la recogida de la información. Se ofertará poner a su disposición la información adicional por otro medio, pero si el interesado solicita alguna aclaración se le deberá ofertar una ***locución complementaria*** con la información adicional correspondiente al epígrafe sobre el que se haya interesado.	Como una locución que se le ofrezca al interesado, como complemento o alternativa a una oferta de disponibilidad de información adicional accesible electrónicamente o remitida, por correo postal o electrónico.

auda
CONSULTORES LOPD y LSSI

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	
Responsable del tratamiento	D./Dña. _____ Nº colegiado _____ Dirección postal _____
Finalidad del tratamiento	Llevar la gestión económica, contable y fiscal del despacho
Plazo de conservación	El plazo de conservación de los datos, será arreglo al que obliga a tener la información contable y fiscal del despacho, ante cualquier requerimiento de la entidad pública competente.
Legitimación	Los datos son tratados en base a la relación que vincula a las partes.
Destinatarios de los datos (cesiones o transferencias)	(indicad si existen terceros que accedan a datos personales o, si por el contrario los datos no son cedidos a ningún organismo o entidad).
Derechos	Ud. podrá ejercitar los derechos de Acceso, Rectificación, Cancelación, Portabilidad, Supresión o, en su caso, Oposición. Para ejercitar los derechos deberá presentar un escrito en la dirección arriba señalada. Deberá especificar cuál de estos derechos solicita sea satisfecho y, a su vez, deberá acompañarse de la fotocopia del DNI o documento identificativo equivalente. En caso de que actuara mediante representante, legal o voluntario, deberá aportar también documento que acredite la representación y documento identificativo del mismo. Asimismo, en caso de considerar vulnerado su derecho a la protección de datos personales, podrá interponer una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

auda
CONSULTORES LOPD y LSSI

3.3. La formalización de servicios prestados por cuenta de los Encargados de Tratamiento) Art 28 RGPD

- **Encargado de Tratamiento =** Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **Posición dual** (Responsable y Encargado) de determinados juristas Ej. Asesor laboral.

3.3.1. Diligencia en la elección y supervisión del Encargado

❑ El Responsable de Tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas. El Encargado ofrecerá conocimientos especializados, fiabilidad y recursos.

❑ Para demostrar que el Encargado (o Subencargado) ofrece garantías suficientes, el RGPD prevé que la adhesión a **CÓDIGOS DE CONDUCTA** o la posesión de un **CERTIFICADO** de protección de datos pueden servir como mecanismos de prueba.

auda
CONSULTORES LOPD y LSSI

3.3.2 ¿Cómo debe regularse la relación entre Responsable y el Encargado ?

- **Contrato o acto jurídico similar** que los vincule.
- Deberá constar **por escrito**, inclusive en formato electrónico.

3.3.3. ¿Cuándo he de articular los contratos o acuerdos de encargo de tratamiento?

Los **contratos de encargo concluidos con anterioridad a la aplicación del RGPD, en mayo de 2018, deben modificarse y adaptarse para respetar este contenido, sin que sean válidas** las remisiones genéricas al artículo del RGPD que los regula Ej. *"Las presentes condiciones y términos estarán conforme al artículo 28 ss RGPD"*.

Vid. directrices para la elaboración de los contratos entre Responsables y Encargados de Tratamiento.
Estas directrices están pensadas para ayudar a responsables y encargados durante el periodo transitorio hasta la entrada en aplicación del RGPD. Posteriormente, y de acuerdo con lo previsto en el Reglamento, la AEPD podrá elaborar clausulados modelo que deberán ser aprobados por el futuro Comité Europeo de Protección de Datos. La Comisión Europea también podrá preparar cláusulas contractuales modelo.

auda
CONSULTORES LOPD y LSSI

3.4 ¿Cuál es el contenido mínimo de un acuerdo o contrato de encargo de tratamiento?

- Objeto, duración y naturaleza
- **Finalidad/es del/los tratamientos.**
- **Tipo de datos** personales y categorías de interesados.
- **Instrucciones** del Responsable.
- Deber de confidencialidad, **secreto profesional.**
- **Medidas de seguridad**, técnicas y organizativas.
- Régimen de **subcontratación** (condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones)
- **Colaboración** en el cumplimiento de obligaciones del Responsable:
  - Comunicación de violaciones de datos.
  - Atención derechos de los interesados.
  - Poner a disposición del Responsable la información necesaria para demostrar el cumplimiento de las obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, realizadas por el responsable o por otro auditor autorizado por el responsable (= Deber de diligencia).
- El **destino de los datos** al finalizar la prestación (conservación, devolución y/o destrucción)

Regularizar también a los prestadores de servicios sin acceso a datos (artículo 83 RDLOPD)

❑ **NO** está recogido en el RGPD.

❑ Pero, por seguridad jurídica aconsejamos que en el contrato de prestación de servicios se recojan las obligaciones a las que están sujetos:

- **Guardar secreto profesional**; obligación que subsistirá aún después de extinguirse la relación con el Responsable y/o Encargado.

- **Prohibición de acceder** a los datos obrantes en papel y a nivel informático.

auda
CONSULTORES LOPD y LSSI

3.4. Las medidas de seguridad en el RGPD

- (Arts 32 RGPDUE). **Medidas de seguridad técnicas y organizativas apropiadas para garantizar un nivel de seguridad apropiado respecto al riesgo**, teniendo en cuenta:

  - ✓ Estado de la técnica,
  - ✓ Costes de aplicación,
  - ✓ Naturaleza, alcance, contexto y fines del tratamiento,
  - ✓ Riesgos para los derechos y libertades de las personas.

- Obligación de incluir una descripción de las mismas **en el registro de actividades de tratamiento «cuando sea posible».**

- La **adhesión a códigos de conducta o mecanismos de certificación** podrá servir de elemento para demostrar el cumplimiento de requisitos de seguridad (art 32.2 RGPDUE).

Accontability o responsabilidad proactiva

❑ Artículo 5.2 RGPD << *El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")* >>

❑ Artículo 24 RGPD << *1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. (= Auditoria).*

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento >>

❑ El principio de *Accountability o Responsabilidad Proactiva* establece una obligación proactiva y sistemática del cumplimiento de la normativa de protección de datos, a través de la implantación de medidas técnicas y organizativas apropiadas; las cuales deberán incluir la protección de datos desde el diseño y por defecto en aquellas áreas de la organización donde sean necesarias. Las diversas políticas o procesos internos de protección de datos o privacidad que deberán ser actualizados y auditados periódicamente.

auda
CONSULTORES LOPD y LSSI

3.5 Notificación de las violaciones, quiebras o brechas de seguridad

* Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos (art 4 RGPD)

A la Autoridad de Control (= alto riesgo para los derechos y libertades)

Deberá realizarse sin dilación indebida y a más tardar en el plazo de 72 horas después de que haya tenido constancia .La comunicación contendrá:

- ✓ Una descripción de la naturaleza de la violación: indicando si es posible las categorías y el número aproximado de interesados afectados.
- ✓ El nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.
- ✓ Una descripción de las posibles consecuencias.
- ✓ Una descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

❖ Asimismo, la violación de seguridad deberá quedar registrada y documentada (= REGISTRO DE INCIDENCIAS).

❖ El Grupo Artículo 29 prepara un formulario estandarizado a nivel europeo, para una notificación armonizada.

A los interesados (= permitir que que puedan tomar medidas para protegerse de las consecuencias)

Se comunicará al interesado sin dilación indebida, la violación de la seguridad de los datos personales, cuando la misma entrañe un alto riesgo para los derechos y libertades de las personas físicas.

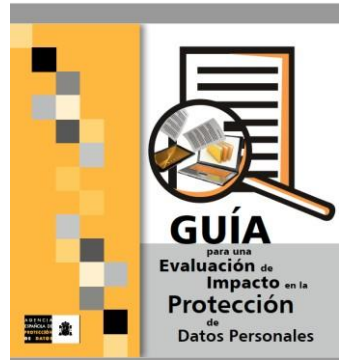
Pérdida de portátil; acceso no autorizado a bases de datos; borrado accidental; exposición pública datos sensibles; usurpación de identidad, etc.

3.6 Evaluación de Impacto relativa a la Protección de Datos (EIPD). ¿Cuándo abordarla?

- Deberá realizarse cuando sea probable que los tratamientos previstos presenten un alto riesgo específico para los derechos y libertades de los interesados .
- Es un proceso más amplio que la mera comprobación del cumplimiento normativo (análisis de riesgos).
- Debe ser sistemática y reproducible.
- Existen supuestos de obligación (art. 35.3 RGPDUE + Considerando 91), supuestos de conveniencia y supuestos de exlusión.
- El RGPD prevé un contenido mínimo de la evaluación (art 35.7 RGPDUE).

AUDA CONSULTORES PERMITE REALIZAR UNA EIPD CONFORME AL RGPD

auda
CONSULTORES LOPD y LSSI



¿ En qué supuestos he de efectuar este análisis de riesgos ?

Supuestos obligatorios (art 35 RGPD)

- ✓ Evaluación sistemática y exhaustiva : Análisis de perfiles.
- ✓ Tratamiento a gran escala relativo a alguna categoría especial de datos.
- ✓ Uso de tecnologías especialmente invasivas como la video vigilancia, biometría, técnicas genéticas, geolocalización, minería de datos etc.
- ✓ Tratamiento grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things), o el desarrollo y la construcción de ciudades inteligentes (Smart Cities).

Es aconsejable que se efectúe una EIPD antes de proceder a determinados tratamientos de datos, en los que vayamos a utilizar nuevas tecnologías y/o concierna a un volumen elevado de datos.
Vid. Guía AEPD sobre las EIPD.

Pero ¿qué entendemos por tratamiento «a gran escala»?

- El WP29 «Directrices sobre el DPO» recomienda considerar los siguientes factores para determinar si el proceso se lleva a cabo a gran escala:
    - Número de interesados (como cifra concreta o como una proporción de la población correspondiente)
    - El volumen de datos
    - La duración o permanencia de la actividad del tratamiento de datos
    - El alcance geográfico de la actividad del tratamiento

- Supuestos exclusión:
    - tratamiento de datos de pacientes por parte de un médico
    - Tratamiento de datos personales relativos a condenas y delitos penales por parte de un abogado

auda
CONSULTORES LOPD y LSSI

Delegado de Protección de Datos (DPO o DPD). Art 37 RGPD

- ¿Cuándo es obligatoria la designación?
  - Administración pública, a excepción de Administración de Justicia.
  - En operaciones de tratamiento que, en virtud de su naturaleza, alcance y/o sus efectos, requieren un seguimiento regular y sistemático a gran escala, de los datos de los titulares.
  - En tratamientos basados en categorías especiales de datos.
- ¿ Quién puede ser DPO ?
  - Puede ser personal interno del centro o externo (= ENCARGADO DE TRATAMIENTO).
  - Especializados del Derecho y, en particular, en materia de protección de datos; si bien, pueden ser de otro perfil.
- Rendirá cuentas directamente al más alto nivel jerárquico de la organización. Autonomía e independencia.

Función: <<*…asignación de responsabilidades, la* ***concienciación y formación del personal que participa en las operaciones de tratamiento****, y las auditorías correspondientes…*>> (artículo 39.b RGPD *in fine*)

Nosotros aconsejamos la formación, sensibilización o concienciación, SIEMPRE.

** Derechos del interesado

Derecho a la Portabilidad [Vid. *Directriz Grupo del artículo 29*]

- Es una forma avanzada del derecho de acceso.
- El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.
- ¿Cuándo?
  - El tratamiento se realice por medios automatizados.
  - Esté basado en el consentimiento o en la ejecución de un contrato.

Derecho de Supresión (= Derecho al Olvido)

- ❑ No está considerado un derecho autónomo o diferenciado de los derechos ARCO, sino es la consecuencia de la aplicación del derecho al borrado. Es una manifestación de los derechos de cancelación u oposición en el entorno on-line.
- ❑ Derecho del ciudadano a solicitar, y obtener de los responsables, sin demora injustificada, que sus datos personales sean suprimidos en el ámbito de Internet:

✓ Derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales.

✓ El responsable del tratamiento, atendiendo a la tecnología disponible y el coste de su aplicación adoptará medidas razonables , incluso medidas técnicas, con el objeto de informar a los responsables correspondientes (supresión de enlaces, copia o réplica).

- ❑ Se prevén límites a su ejercicio.

Disposiciones generales derechos A.R.C.O

❑ **Gratuidad:** **no obstante, se establecen** los **supuestos** en los **que** el Responsable **puede cobrar una tasa o canon** razonable o incluso negarse a responder. Ej. solicitudes abusivas que manifiestamente infundadas, excesivas, o aquellas que tengan un carácter repetitivo.

❑ **Plazos:** se establece un plazo de **1 MES para hacer efectivo el derecho del interesado**, el cual puede ser prorrogado por 2 meses más en supuestos de complejidad o número de solicitudes recibidas.

❑ **Medios Electrónicos:** Se debe proporcionar medios para que las solicitudes se presenten por medios electrónicos.

❑ **Negativa a la solicitud:** en los supuestos en los que no se le conceda el ejercicio de derechos deberá ser informado en el mismo **plazo de un mes de los motivos y la posibilidad** de presentar la correspondiente **reclamación ante la Autoridad** competente.

❑ **Información adicional:** en aquellos casos en los que existan dudas razonables sobre la identidad de la persona física que realiza la solicitud.

auda
CONSULTORES LOPD y LSSI

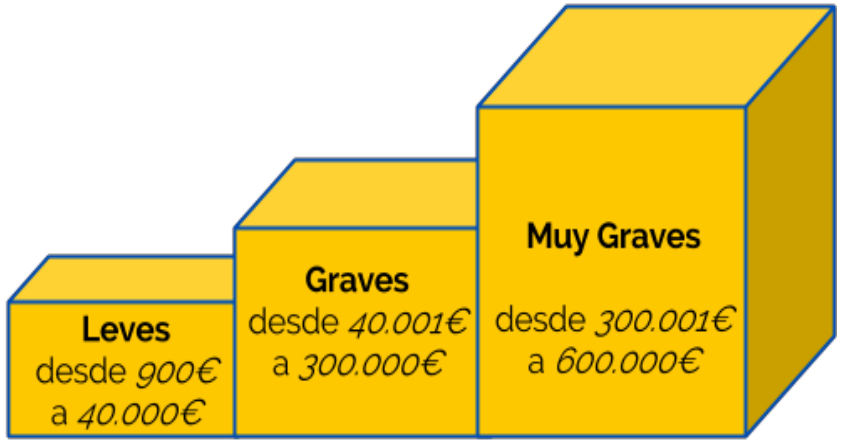
** Auditoria

- **No** se fija de forma obligatoria con un **plazo temporal**.
- En el RGPD nos encontramos diferentes **alusiones, directas o indirectas**, a esta obligación:
  - «*verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*»
  - La función del DPO de supervisar «*las auditorías correspondientes*»
  - El deber del Encargado de Tratamiento de «*permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable*».
  - Sanción

Por tanto, **es pertinente continuar sometiendo las medidas de seguridad a Auditoria**.

auda
CONSULTORES LOPD y LSSI

4) RÉGIMEN SANCIONADOR



- NO contempla una graduación de sanciones (leve, grave y muy grave).
- Pensado más para aplicar a grandes corporaciones.

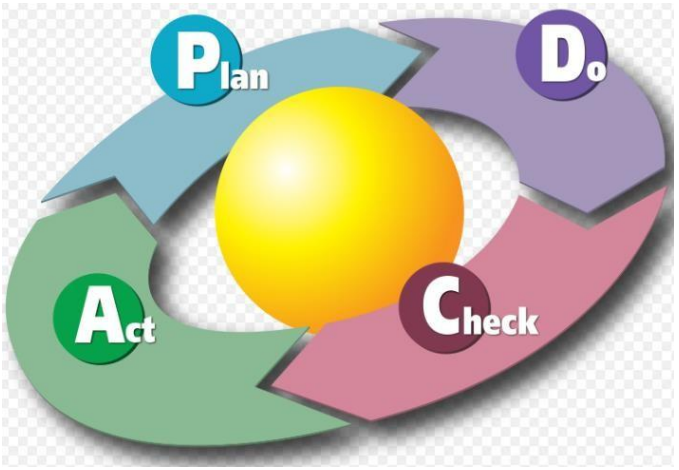
10 millones de euros	2% Volumen negocio
20 millones de euros	4% Volumen negocio

auda
CONSULTORES LOPD y LSSI

¿VALE LA PENA CORRER EL RIESGO? NO, GRACIAS

auda
CONSULTORES LOPD y LSSI

A trabajar… Quiero adecuarme al RGPD pero ¿por dónde empiezo?



FASE - PLAN

- ✓ Definición de responsables. DPO/R.Seguridad, etc...
- ✓ Inventario de tratamientos
- ✓ Análisis de necesidad/ conveniencia EIPD
- ✓ Realización de EIPD (con funciones de Plan de tratamiento)

FASE - DO

- ✓ Implantación de controles:
  - ✓ Jurídicos (Cláusulas, Contratos)
  - ✓ Técnicos (Medidas de Seguridad)
  - ✓ Organizativos (Procedimientos diversos)

FASE - REVISIÓN (CHECK)

- ✓ Controles periódicos
- ✓ Auditorías

FASE - MEJORA CONTINUA (ACT)

- ✓ No Conformidades
- ✓ Acciones Correctivas
- ✓ Planes de Mejora

MUCHAS GRACIAS POR LA ATENCIÓN

auda

CONSULTORES LOPD y LSSI