

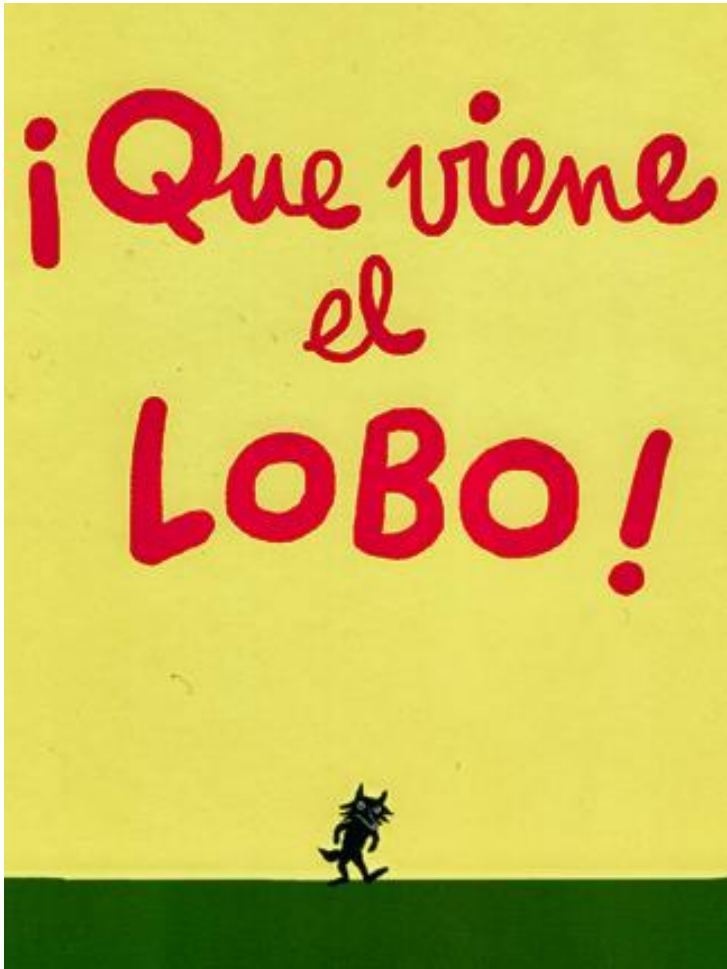
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD)

Eugenio Fernández
Universidad de Alcalá

Introducción



Introducción



Ley Orgánica 15/**1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal (***vigente en aquellos artículos que no contradigan el RGPD***)



Introducción



Real Decreto 1720/**2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (***vigente en aquellos artículos que no contradigan el RGPD***)



NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS

Introducción



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)

Real Decreto-ley 5/**2018**, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD)

Introducción al concepto de Protección de Datos

Introducción al concepto de Protección de Datos

Protección

**Gestión adecuada,
Seguridad**



Datos

**Datos, Información,
Perfiles, ..., por Niveles**



Personales

De personas, no empresas



Introducción al concepto de Protección de Datos



Intimidad, Privacidad y Protección de Datos de Carácter Personal

Intimidad, Privacidad y PDCP



No todo lo privado es íntimo pero todo lo íntimo es privado.

No todos los datos personales son íntimos o privados, pero **todos son susceptibles de protección.**

Intimidad, Privacidad y PDCP



Privacy: EE.UU.

- ♦ No es un derecho constitucional:
- ♦ Definido poco a poco por la doctrina y la jurisprudencia
- ♦ "The right to be let alone"
- ♦ No hay Ley de protección de datos federal
- ♦ "Políticas de Privacidad": El dueño de los datos es la empresa

Privacidad: U.E.

- ♦ Es un derecho constitucional distinto de la intimidad.
- ♦ Es el derecho a la protección de datos personales.
- ♦ Hay Directiva Europea de Protección de Datos y LOPD
- ♦ Requisitos y sanciones.
- ♦ El dueño de los datos es la persona.

Marco Legal

Marco Legal

- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente en aquellos artículos que no contradigan el RGPD)
- **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD)
- **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)
- **Real Decreto-ley 5/2018, de 27 de julio**, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD)**

Principios Básicos



Principios Básicos

Básicos

CONOCIMIENTO

De todo el ciclo de vida del dato y protegerlo en cada momento, desde la captación a la destrucción.

COMPROMISO

Con los derechos de quienes te confían sus datos.
Con los deberes a los que estas sujeto.

TRANSPARENCIA

Muchísima mayor transparencia en la gestión de los datos personales.



Principios Básicos

Según el art. 5, RGPD, los datos deberán

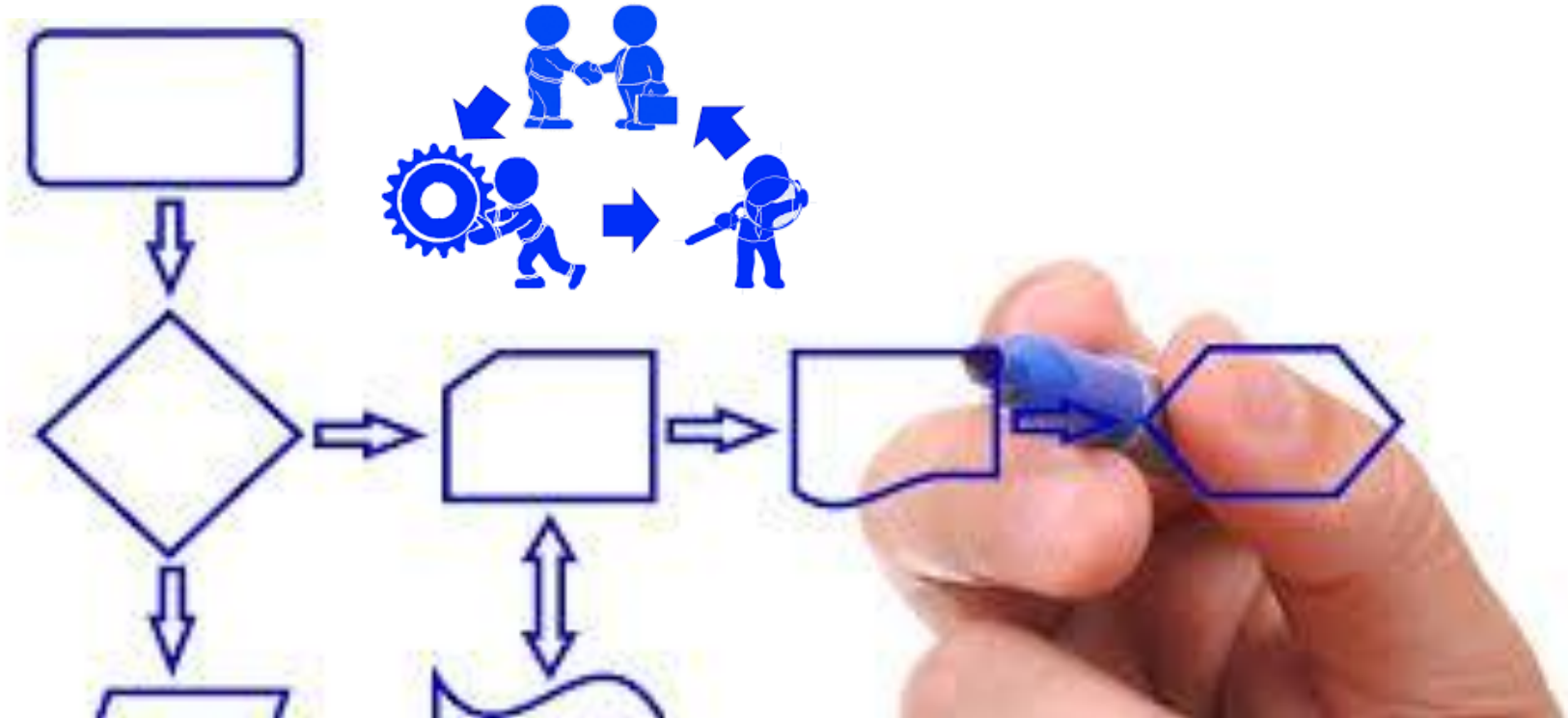
- a) Ser tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
- b) Ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;
- c) Ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
- d) Exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
- e) Ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales;
- f) Ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

La PDCCP como proceso

La PDGP como proceso



Enfoque orientado a procesos



La PDCP como proceso

¿CÓMO CUMPLIR EL RGPD Y LA LOPD?



<https://ayudaleyprotecciondatos.es>

AYUDALEYPROTECCIONDATOS.ES

Privacy by Design



Privacy by Design

Importante cambio de enfoque del RGDP

Privacidad desde el Diseño o “Privacy by Design”

- **Enfoque anterior:** abordar la implementación de la PD al final del proceso de desarrollo de un servicio, un producto, etcétera.
- **Enfoque actual:** abordar la implementación de la PD en el momento del **diseño** de un servicio, un producto, etcétera.

Este concepto no lo encontramos en un artículo en concreto sino que se hace mención a él en diferentes apartados del RGPD. Por ejemplo:

Considerando 78 del RGPD

“...A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto...”

Accountability



Accountability

Principio de “accountability” o principio de responsabilidad activa

- Una entidad no solo tiene que cumplir con la normativa de protección de datos, sino que tiene que demostrar que la cumple.
- Hay que tener responsabilidad proactiva tanto en el cumplimiento como en su demostración.
- El responsable se encuentra obligado a aplicar medidas organizativas y técnicas que sean apropiadas para, no solo garantizar, sino también poder demostrar, que el tratamiento de los datos se realiza conforme a la normativa.

Accountability

Principio de “accountability” o principio de responsabilidad activa

El Responsable del Tratamiento deberá:

- Adoptar Medidas de protección de datos desde el diseño y por defecto (**Privacy by design**).
- Realizar un **Análisis de Riesgos** y adopción de medidas de seguridad
- **Notificar las quiebras de seguridad**
- Realizar **Evaluaciones de Impacto** sobre la protección de datos
- Fomentar la adhesión por parte de responsables y encargados de tratamiento a **códigos de conducta, mecanismos de certificación, sellos y marcas de protección de datos.**

Códigos de Conducta



Códigos de Conducta

Los códigos de conducta especificarán la aplicación del Reglamento a las características y necesidades de los distintos sectores de actividad, pymes o micropymes.

Sirven para adecuar la aplicación del RGPD a las características de los distintos sectores de actividad y además,

- Pueden servir de elemento para demostrar el cumplimiento de las obligaciones de los responsables
- Pueden servir de elemento para demostrar el cumplimiento de las obligaciones sobre medidas de seguridad (para responsables y encargados)
- Se tendrán en cuenta a efectos de evaluar el impacto en protección de datos de las operaciones de tratamiento –PIAS- (para responsables y encargados)
- Pueden servir de elemento para demostrar que el encargado adherido a un código ofrece garantías suficientes (para encargados o subencargados)
- Pueden servir para aportar garantías suficientes para realizar transferencias internacionales de datos (en este caso su tramitación también requerirá el dictamen del CEPD)
- Se tendrán en cuenta en la determinación de sanciones.

BCR



BCR

Normas Corporativas Vinculantes (BCR-Binding Corporate Rules)

"Son políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta".

La autoridad de control competente aprobará normas corporativas vinculantes (más conocidas por sus siglas en inglés BCR -Binding Corporate Rules-) de conformidad con el mecanismo de coherencia establecido en el artículo 63 del RGPD.

Lista Robinson



Lista Robinson

La Lista Robinson es un servicio que sirve para que podamos excluir la publicidad que no deseamos. Para su adaptación al nuevo Reglamento General de Protección de Datos, han colaborado tanto la Agencia Española de Protección de Datos (AEPD) como la Asociación Española de Economía Digital (Adigital).

The screenshot shows the homepage of the Lista Robinson website. At the top, there is a navigation bar with the 'Lista Robinson' logo on the left and links for 'Inicio', '¿Qué es?', 'Reglamento', 'Empresas', and an 'Acceder' button on the right. The main content area has a blue background with the heading 'Evita la publicidad no deseada' in white. Below the heading, a paragraph explains that the service allows users to easily and free of charge avoid advertising from companies they are not clients of or have not given consent to. It also mentions that the service works for phone, postal, email, and SMS/MMS advertising. At the bottom of this section is a large white button with the text 'APÚNTATE EN LA LISTA' in blue.

Lista Robinson

[Inicio](#) [¿Qué es?](#) [Reglamento](#) [Empresas](#) [Acceder](#)

Evita la publicidad no deseada

El Servicio de Lista Robinson te permite, de forma fácil y gratuita, evitar publicidad de empresas de las que no seas cliente o a las que no hayas facilitado tu consentimiento. Funciona para publicidad por teléfono, correo postal, correo electrónico y SMS/MMS.

[APÚNTATE EN LA LISTA](#)

Dato de Carácter Personal

Dato de carácter personal

*“Cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a **personas físicas vivas identificadas o identificables**”.*

- *Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*
- *La imagen de una persona es un dato personal, al igual que lo será cualquier información que permita determinar, directa o indirectamente, su identidad, como por ejemplo, una matrícula de vehículo, una dirección IP, etc.*
- *Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.*

Dato de carácter personal

*“Cualquier información concerniente a **personas físicas vivas** identificadas o identificables”.*

- *Es independiente la tecnología utilizada para su tratamiento (**neutralidad tecnológica**).*
- *Se aplica tanto al tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados (como el orden alfabético).*
- *No importa cómo se “almacenan” los datos: sistema informático, transmisión en vivo (**videovigilancia**), papel, etcétera.*

Dato de carácter personal

*“Cualquier información concerniente a **personas físicas vivas** identificadas o identificables”.*

- *Los datos personales que hayan sido **anonimizados** pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales.*
- *Los datos personales que hayan sido **anonimizados**, de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales.*



Dato de carácter personal

Son (o pueden llegar a ser) datos de carácter personal:

- *nombre.apellido@empresa.com*
- *Datos de localización (e.g. teléfono móvil)*
- *Dirección de protocolo de internet (IP)*
- *El identificador de una cookie*

Dato de carácter personal

Datos de Contactos

- Información referida a personas físicas identificadas (datos de carácter personal): su tratamiento se encuentra sometido al RGPD.
- Por tanto, desaparece la exclusión que recogía el Reglamento de desarrollo de la LOPD de 1999.
- No obstante, su tratamiento podría realizarse al amparo del artículo 6.1 f) del RGPD (regla del interés legítimo) si se cumplen los siguientes requisitos:
 - Se traten los mínimos datos imprescindibles de contacto.
 - Se traten con la finalidad de mantener relaciones "business to business" (B2B)
- Se entenderán incluidos los cargos de la persona, su nivel de responsabilidad, posición física dentro de la organización, teléfono de contacto fijo, teléfono móvil corporativo, mail corporativo e incluso redes sociales corporativas en el caso de que se utilicen para la promoción de la organización.
- No podemos incluir los números de teléfonos privados, aunque se utilicen en el ámbito laboral, o los correos personales que se utilizan en el ámbito profesional.

Dato de carácter personal

Datos de Empresarios Individuales (Autónomos)

- Información referida a personas físicas identificadas (datos de carácter personal): su tratamiento se encuentra sometido al RGPD.
- Por tanto, también desaparece la exclusión que recogía el Reglamento de desarrollo de la LOPD de 1999.
- No obstante, también su tratamiento podría realizarse al amparo del artículo 6.1 f) del RGPD (regla del interés legítimo) si se cumplen los siguientes requisitos:
 - Siempre y cuando se refieran a los empresarios individuales en dicha condición.
 - No se traten para entablar una relación con los mismos como personas físicas.)

Seudonimización

Seudonimización

Anonimización (Disociación)

- Es el proceso por el cual los datos se eliminan de manera irreversible.
- Con la anonimización, el dato personal se disociará por completo, por lo que un sujeto no podrá ser identificado.
- Desde ese momento, su tratamiento no entraría dentro del ámbito del Reglamento General de Protección de Datos.
- Hay que saber muy bien cómo realizarlo y cuándo se puede llevar a cabo. El artículo 9 del RGPD recomienda la existencia de un equipo para el estudio de la viabilidad del proceso de anonimización, especialmente si se trata de datos protegidos.

Orientaciones y
garantías
en los
procedimientos de
ANONIMIZACIÓN
de datos
personales



Seudonimización

Seudonimización

- Información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- Medida que puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos a los datos personales.
- Solo reemplaza parte del conjunto de datos y no permite la identificación directa del sujeto. Sin embargo, se puede averiguar la identidad del sujeto a través de informaciones adicionales. Por tanto, la seudonimización está sujeta al RGPD.

Seudonimización

Seudonimización: objetivos

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Cumplir con mayor facilidad con ciertas exigencias del nuevo Reglamento y con uno de los mayores retos incluidos en el mismo, el del control del riesgo.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico (uno de los significados de resiliencia).
- Implantar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Seudonimización

Seudonimización

Mecanismos de seudonimización más frecuentes (Dictamen 05/14 del Grupo de Trabajo sobre Protección de Datos de Carácter del artículo 29):

- Cifrado con clave secreta
- Función hash
- Función con clave almacenada
- Cifrado determinista
- Función hash con clave de borrado de clave
- Descomposición en tokens.



Conceptos Asociados

Fichero

Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

La pura acumulación de datos que comporte una búsqueda, acceso e identificación muy complicada no puede ser considerado “fichero” a los efectos que nos ocupan.

Atendiendo a esta definición se pueden distinguir **tres tipos de ficheros**: los informatizados, los no informatizados -denominados también “ficheros manuales”-, y los ficheros mixtos – parte informatizado, parte manual-.

Inscripción (Declaración de Ficheros

Inscripción de ficheros

Aviso a responsables

Con motivo de la próxima aplicación del Reglamento General de Protección de Datos, que suprime la obligación de notificar ficheros a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos, el día 14 de mayo de 2018 dejan de estar operativos los sistemas de notificación de ficheros tanto a través del formulario NOTA como a través del envío de notificaciones en formato XML.

La obligación de notificar ficheros se sustituye a partir del 25 de mayo de 2018 por elaborar un registro de actividades de tratamiento que deberá contener la información señalada en el artículo 30 del citado Reglamento.

Interesado

“Persona física titular de los datos que sean objeto del tratamiento”.

Se debe tener en cuenta que no es necesario que la persona física esté plena y actualmente identificada, **basta con que sea identificable**; y, de otra parte, que sólo pueden ser afectados las personas físicas, ya que **la protección de datos “personales” no afecta a los datos de las personas jurídicas**.



Destinatario o cesionario

“Persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos”.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Tercero

Persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Asimismo, pueden tener también la condición de terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Ficheros de titularidad pública

Son los ficheros de los que sean responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a las mismas, las Administraciones Públicas Territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.



Ficheros de titularidad privada

Son los ficheros de los que sean responsables las personas, empresas o entidades sometidas al derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentran estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.



Fuentes accesibles al público

Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Las fuentes de acceso público se encuentran enumeradas y tasadas en la LOPD:

- El censo promocional
- Los repertorios telefónicos
- Listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, los Diarios y Boletines Oficiales y los medios de comunicación social.
- Internet no es fuente de acceso público

A día de hoy, con el RGPD en vigor, no puede hablarse de un concepto legal de «fuentes accesibles al público» como el que existía en la LOPD



Deber de Secreto

Cualquier persona que intervenga en el tratamiento de datos de carácter personal está obligado al secreto profesional.

Dicho secreto deberá guardarse incluso después de haber finalizado su relación con el titular del fichero.



Calidad de los Datos

Los datos de carácter personal sólo se podrán recoger para su tratamiento y tienen que ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

- *No podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos.*
- *Los datos serán exactos y actualizados en todo el momento.*
- *Si son inexactos, serán cancelados o sustituidos por los correspondientes datos rectificados o completados.*
- *La rectificación y cancelación notificada tiene que resolverse y notificarse al cesionario en el plazo de 10 días.*
- *Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados.*
- *Podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una obligación jurídica o de ejecución de un contrato, etc. Una vez cumplido este período, sólo podrán ser conservados previa disociación de los mismos.*
- *Los datos de carácter personal serán almacenados de forma que permitan el ejercicio de derecho de acceso, salvo que sean legalmente cancelados.*
- *Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.*

Tratamiento de datos

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.

Tratamiento de datos

Interés Legítimo

- Se establecen, en el artículo 6, apartado 1º, del RGPD, una serie de legitimaciones, de tal forma que, basándose en cualquiera de ellas, el tratamiento que realice el Responsable, será legítimo.
 - Consentimiento expreso del interesado.
 - Existencia de un contrato o precontrato entre las partes.
 - Obligación de cumplir con un deber establecido legalmente.
 - Protección del interés vital, tanto del afectado como de terceras personas.
 - Concurrencia de un interés público o ejercicio de poderes públicos por el Responsable del Tratamiento.



Cesión de datos

Toda revelación de datos realizada a una persona distinta del interesado.

Hay que distinguir entre:

- La **cesión de datos** propiamente dicha
e.g. Vender los datos de clientes de una empresa a otra.
- El **acceso a datos por cuenta de un tercero** para la prestación de un servicio.
e.g. Dar acceso a los datos de los empleados por parte de una empresa a otra, para que la segunda pueda realizar operaciones por encargo de la primera (realizar las nóminas).

Cesión de Datos

Requisitos para la cesión de datos (al menos una de ellas):

- Consentimiento de los titulares de los datos.
- Cesión necesaria para el desarrollo de una relación contractual (e.g. contrato de la luz).
- Cesión obligatoria legalmente para el cedente (e.g. datos a las fuerzas de seguridad).
- Cesión que obedezca a intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.
- Cesión necesaria para salvaguardar el interés vital del interesado o de otras personas (e.g. en caso de accidente).

Derechos

Derechos



Miguel Solano Gadea

@solanogadea

Seguir



Me proponen el acrónimo **#SOPLAR** para sintetizar los derechos del **#RGPD** (2016/679) sin conservar el orden de enunciado. Hoy **#ARCO** en **#LOPD**

LOPD actual (1999 y hasta 05.2018) y Directiva 95/46/CE



MSG
2017.07



LOPD futura 05.2018 y Reglamento General (UE) 2016/679

Derechos

Derecho de Acceso: solicitar información sobre el tratamiento de los datos.

- No es necesario justificarlo si no se ha ejercido en los últimos 12 meses.
- El plazo máximo para la resolución es de **30 días**.
- Tras la comunicación, 10 días hábiles para realizar el acceso.

Derecho de Rectificación: solicitar la modificación de datos que sean inexactos o incompletos.

- Debe justificarse.
- 10 días hábiles para llevar a cabo la resolución

Derecho de Oposición: al tratamiento de sus datos personales o el cese de éstos en determinados casos, con motivos fundados y legítimos.

- *Que no sea necesario su consentimiento.*
- *En los que los ficheros se usen con finalidades publicitarias.*
- *El tratamiento tenga por finalidad la adopción de una decisión referida al afectado.*
- 10 días hábiles para llevar a cabo la resolución.

Derechos

Derecho a la limitación del tratamiento: limitación del tratamiento de los datos.

Cuando:

- El interesado impugne la exactitud de los datos.
- El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- El responsable ya no necesite los datos personales para los fines del tratamiento.
- El interesado se haya opuesto al tratamiento y mientras se verifica si los motivos

Derecho a la portabilidad de los datos: posibilidad de solicitar al responsable del tratamiento que se le faciliten los datos personales en un formato estructurado y claro a otro responsable..

Derecho al olvido o supresión: supresión de los datos personales del interesado sin dilación. Se podrá ejercer cuando dichos datos:

- Ya no sean necesarios conforme a su finalidad.
- Se retire el consentimiento.
- Se ejerza el derecho a oposición sobre los mismos.
- Sean tratados de forma ilícita.

Derechos

Sobre los derechos

- Su ejercicio es gratuito.
- Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter repetitivo) el responsable podrá cobrar un canon o negarse a actuar.
- Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más.
- El responsable está obligado a informarte sobre los medios para ejercitar estos derechos.
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.
- Puedes ejercer los derechos directamente o por medio de tu representante legal o voluntario.
- Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule.



Reutilice la Información de la Agencia

Deber de Información al interesado o usuario



Deber de Información

El deber de informar está íntimamente relacionado con el concepto de consentimiento, que en el RGPD tiene que ser explícito.

Cualquier empresa u organización que trate con datos personales ha de hacer saber al usuario que los va a utilizar, la forma y las opciones que tiene de ejercer sus derechos.



Deber de Información

¿Quién debe informar?

- **Responsable del Tratamiento**
- **Encargado del Tratamiento** si es este quien recoge los datos

¿Cuándo se debe informar?

- **Si la información se obtiene del propio interesado:** en el momento en que se soliciten y recojan los datos.
- **Si la información no se obtiene del propio interesado:** dentro de un plazo razonable, pero en cualquier caso dentro de un mes.

Deber de Información

¿Cuándo no es preciso informar?

- Los datos procedan del interesado y el interesado ya disponga de la información.
- Los datos no procedan del interesado y:
 - *El interesado ya disponga de toda la información legalmente exigible.*
 - *La comunicación resulte imposible o suponga un esfuerzo desproporcionado.*
 - *La obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros.*
 - *Cuando los datos deban seguir teniendo carácter confidencial por una obligación legal de secreto profesional, incluida una obligación de secreto de naturaleza estatutaria.*

Deber de Información

¿Cómo se debe informar?

- En un lenguaje claro y sencillo.
- De forma concisa, transparente, inteligible y de fácil acceso.
- Se debe buscar un equilibrio entre concisión y precisión, evitando circunloquios, explicaciones innecesarias o detalles confusos.
- Se debe evitar el abuso de citas legales innecesarias y términos ambiguos o con escaso sentido para las personas destinatarias.
- Cuando los destinatarios sean menores, debe utilizarse un lenguaje adecuado a su nivel de comprensión.
- **Se recomienda una información por capas**



Deber de Información

Información por capas

- Presentar una información básica (información resumida) en un primer nivel, de manera que permita tener un conocimiento general del tratamiento.
- Ofrecer el resto de la información adicional (información detallada) en un segundo nivel

Deber de Informació

Información por capas

Información obtenida directamente del interesado

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, incluida, en su caso, la existencia de decisiones automatizadas y la elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Lógica aplicada en la elaboración de perfiles y consecuencias previstas
"Legitimación"	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 los datos y consecuencias de no hacerlo
		Posibilidad de retirar el consentimiento, en su caso
"Destinatarios"	Previsión o no de cesiones	Destinatarios o categorías de destinatarios
	Previsión de transferencias, o no, a terceros países	Decisiones de adecuación, garantías y medios para obtener copia de datos, o situaciones específicas aplicables
"Derechos de las personas interesadas"	Referencia a la posibilidad de ejercicio de los derechos de acceso, rectificación, supresión y portabilidad, y la limitación u oposición a su tratamiento	Cómo ejercer los derechos: información general sobre los distintos derechos, canales para ejercerlos, enlaces a formularios
		Derecho a reclamar ante la autoridad de control
		Categorías de datos que se tratan

NUEVO

Deber de Información

Información por capas

Información no obtenida del interesado

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, incluida, en su caso, la existencia de decisiones automatizadas y la elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Lógica aplicada en la elaboración de perfiles, consecuencias previstas y derecho a oponerse
"Legitimación"	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 los datos y consecuencias de no hacerlo
		Posibilidad de retirar el consentimiento, en su caso
"Destinatarios"	Previsión o no de cesiones	Destinatarios o categorías de destinatarios
	Previsión de transferencias, o no, a terceros países	Decisiones de adecuación, garantías y medios para obtener copia de datos, o situaciones específicas aplicables
"Derechos de las personas interesadas"	Referencia a la posibilidad de ejercicio de los derechos de acceso, rectificación, supresión y portabilidad ¹ , y la limitación u oposición a su tratamiento	Cómo ejercer los derechos: información general sobre los distintos derechos, canales para ejercerlos, enlaces a formularios
		Derecho a reclamar ante la autoridad de control
"Categorías de datos"	Si se tratan o no categorías especiales de datos o datos relativos a condenas e infracciones penales	Categorías concretas de datos tratados
"Procedencia de los datos"	Fuente de los datos	Información detallada del origen de los datos. Si procedan de fuentes de acceso público, deberá concretarse la fuente

Deber de Información

Información por capas

Información básica sobre protección de datos	
Responsable	Ediciones Warren&Brandeis, S.A. +info...
Finalidad	Gestionar el envío de información y prospección comercial +info...
Legitimación	Consentimiento del interesado +info...
Destinatarios	Otras empresas del grupo Warren&Brandeis, Inc., encargados de tratamiento fuera de la UE acogidos a "Privacy Shield" +info...
Derechos	Acceder, rectificar y suprimir los datos, solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de éste +info...
Información adicional	Puede consultar la información adicional y detallada sobre protección de datos en nuestra página web

Deber de Información

Información por capas

Ejemplo de información básica en entrevista telefónica

En una entrevista telefónica, antes de proceder a la recogida de la información, se deberá ofrecer la información básica como un **mensaje claro y conciso**, pero asegurando que el interlocutor la haya comprendido.

Se ofrecerá poner a su disposición la información adicional por el mismo u otro medio, pero si el interesado solicita alguna aclaración se le deberá ofrecer un **mensaje complementario** con la información adicional correspondiente al epígrafe o epígrafes sobre los que se haya interesado.

En este caso, las personas operadoras del servicio deberán estar en disposición de atender las solicitudes de aclaración o ampliación de la información ofrecida.

Información adicional telefónica:

- ✓ Como una locución que se ofrezca al interesado, como complemento a una oferta de disponibilidad de información adicional accesible electrónicamente.

Deber de Información

Información por capas

Ejemplo: **¿Quién es el responsable del tratamiento de sus datos?**

Identidad: Ediciones Warren&Brandeis, S.A.

Dir. postal: Calle Universidad de Harvard, nº. 5 - 28000 Madrid

Teléfono: 912345678

Correo electr.: info@warrenbrandeis.com

Delegado de protección de datos: Calle Universidad de Harvard, nº. 6 - 28000 Madrid (dpd@warrenbrandeis.com)

Contacto DPD: <https://www.warrenbrandeis.com/protecciondatos/dpd/>

Deber de Información

Información por capas

Ejemplo: ¿Cuál es la legitimación para el tratamiento de sus datos?

“La base legal para el tratamiento de sus datos es la ejecución del contrato de suscripción a las revistas que figuran en su cartera de pedidos (... según los términos y condiciones que constan en ...)”

Si ha marcado la casilla correspondiente, la base legal para el envío de publicidad sobre otros productos y servicios es su consentimiento, que puede retirar en cualquier momento, sin que la retirada del consentimiento para esta finalidad condicione la ejecución del contrato de suscripción.”

Deber de Información

Información por capas

Ejemplo:

¿Con qué finalidad tratamos sus datos personales?

"En Warren & Brandeis tratamos la información que nos facilitan las personas interesadas con el fin de (...gestionar el envío de la información que nos soliciten.../...facilitar a los interesados ofertas de productos y servicios de su interés.../...)"

"Con el fin de (... poder ofrecerle productos y servicios de acuerdo con sus intereses... / mejorar nuestros servicios...), elaboraremos un perfil comercial, a partir de la información facilitada. No se tomarán decisiones automatizadas en base a dicho perfil."

¿Cuánto tiempo conservaremos sus datos?

"Los datos personales proporcionados se conservarán (...mientras se mantenga la relación mercantil .../... no se solicite su supresión por el interesado.../...durante un plazo de xx años a partir de la última confirmación de interés...)"

Deber de Información

Información por capas

Ejemplo: ¿A qué destinatarios se comunicarán sus datos?

“Los datos se comunicarán a otras empresas del grupo empresarial Warren&Brandeis, Inc. para fines administrativos vinculados al tratamiento de datos personales de clientes o empleados”.

“Warren&Brandeis, Inc. dispone de normas corporativas vinculantes, aprobadas por el Comité Europeo de Protección de Datos y disponibles en: <https://www.warrenbrandeis.com/protecciondatos/bcr/> .

“Warren&Brandeis S.A. contrata su infraestructura virtual según un modelo de computación en la nube a través de AWS y al amparo del acuerdo EU-US Privacy Shield. Información disponible en:

<https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4> .

Deber de Información

Información por capas

- Ejemplo:

¿Cuáles son sus derechos?

- Cualquier persona tiene derecho a obtener confirmación sobre si en Warren&Brandeis estamos tratando datos personales que les conciernan, o no.
- Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.
- En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.
- Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. Warren&Brandeis dejará de tratar los datos, salvo por motivos legítimos imperiosos o el ejercicio o la defensa de posibles reclamaciones.
- En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

Deber de Información

Información por capas

¿Cómo se pueden ejercer los derechos?

- Mediante un escrito dirigido a Ediciones Warren&Brandeis, S.A., C/ Universidad de Harvard, nº. 5 - 28000 Madrid.
- Mediante el formulario electrónico disponible en <https://www.warrenbrandeis.com/protecciondatos/dpd/>

¿Qué vías de reclamación existen?

- Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante ... (indicar la autoridad de protección de datos competente).

Deber de Información

Información por capas

Ejemplo: ¿Qué categorías de datos tratamos?

- Datos identificativos
- Características personales
- Datos académicos
- Información laboral
- Información económico-financiera

No se tratan categorías especiales de datos.

Deber de Información

Información por capas

Ejemplo: **¿Cómo hemos obtenido sus datos?**

Los datos personales que tratamos proceden de otras empresas del grupo Warren&Brandeis Inc.

Consentimiento

Consentimiento

Concepto

“El consentimiento es 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 datos personales que le conciernen”.

El 28 de noviembre de 2017, el Grupo publicó el borrador de Directrices sobre el consentimiento bajo el Reglamento General de Protección de Datos para facilitar la comprensión del término “consentimiento” en virtud del Reglamento 2016/679.

Consentimiento

El RGPD exige que el consentimiento sea libre, específico, informado e inequívoco (consentimiento **inequívoco**).

El consentimiento podrá obtenerse mediante una declaración o mediante una acción afirmativa (incluyendo el consentimiento **inferido**).

En los supuestos legalmente exigibles, deberá facilitarse de forma explícita (consentimiento **explícito**).

Consentimiento

Tipos de Consentimiento



NO constituirán un consentimiento válido

- **Casillas ya marcadas por defecto.**
- El consentimiento **tácito** (resultará de hechos o de actos que lo presupongan o que autoricen a presumirlos).
- La **inacción del usuario.**
- El consentimiento **por omisión.**

Consentimiento

Tipos de Consentimiento

CONSENTIMIENTO INEQUÍVOCO IMPLÍCITO

- El interesado prestará el **consentimiento mediante una declaración inequívoca o una acción afirmativa clara**.
- **El interesado tiene que hacer algo, y ese algo que solo puede ser interpretado como que acepta el tratamiento.**
 - e.g. el acceso a una zona videovigilada con un cartel que informa de la existencia de cámaras.
- Si la acción del usuario se puede interpretar de varias maneras, no podríamos deducir el consentimiento del mismo.

Consentimiento

Tipos de Consentimiento

CONSENTIMIENTO EXPLÍCITO O EXPRESO

Una clara acción afirmativa (“Sí acepto ☐”) no implica, necesariamente, el consentimiento expreso (concepto del consentimiento inferido, que permite la manifestación del consentimiento del interesado a través de un determinado comportamiento del que se infiera esa voluntad de consentir).

El interesado debe dar una declaración expresa de consentimiento (e.g. firma)

El Reglamento señala que podría ser necesario un consentimiento expreso para tratar los siguientes datos:

- Para categorías especiales de datos
- Para transferencias internacionales de datos a un tercer país u organización internacional
- Para la toma de decisiones individuales automatizadas que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar

Consentimiento

Tipos de Consentimiento

CONSENTIMIENTO EXPLÍCITO O EXPRESO

Ejemplos (Guideline del WP29)

- Confirmación del consentimiento a través de una declaración escrita.
- Firma de una declaración escrita.
- El envío de una declaración rellenando un formulario electrónico.
- El envío de una declaración vía correo electrónico.
- La subida de un documento firmado escaneado.
- El uso de firma electrónica.
- Posibilidad de otorgarlo verbalmente, pero dificultad en la prueba.

Una forma de asegurarse de que el consentimiento explícito es válido es utilizando una verificación en dos pasos utilizar la verificación en dos pasos con el objetivo de asegurarse que se obtiene un consentimiento explícito lícito (e.g. correo de solicitud de tratamiento de datos + respuesta con “Acepto” + correo con link o SMS para verificación).

Consentimiento

Tipos de Consentimiento

El consentimiento, además de INEQUÍVOCO, ha de ser EXPLÍCITO:

- Tratamiento de datos sensibles.
- Adopción de decisiones automatizadas.
- Transferencias internacionales.

El consentimiento puede ser INEQUÍVOCO y otorgarse de forma IMPLÍCITA:

- Cuando se deduzca de una acción del interesado.
- e.g. el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación.

Consentimiento

Tipos de Consentimiento

e.g. Seguir navegando en una web sin aceptar cookies

AEPD “Guía para Responsables del Tratamiento” de enero del 2017.

El consentimiento *puede ser inequívoco y otorgarse de forma implícita* cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).

Directrices sobre el Consentimiento del Grupo de Trabajo del art 29

El mero hecho de seguir utilizando la web (scroll down o seguir ojeando la página) no satisface los nuevos requisitos del consentimiento (en el sentido comentado de acción clara y afirmativa).

Y ello porque ese supuesto consentimiento manifestado en “seguir navegando” no se distingue de forma suficientemente clara de la conducta de quien no ha reparado en el banner de cookies, ni ha leído su contenido, y sigue leyendo el texto de la web.

Consentimiento

Objetivo en términos prácticos

Recabar (por parte del responsable del fichero o del tratamiento) el consentimiento de la forma más sencilla de forma que no afecte negativamente a los proceso de negocio (e.g. rechazo del usuario).



LEXblogger

Consentimiento

Cómo debe hacerse

- Introducir una cláusula completa informando y solicitando aceptación.
- La información que hay que proveer a los interesados:
 - La necesidad del tratamiento de datos, así como de la finalidad y temporalidad (por cuánto tiempo van a tratarse los datos).
 - Los derechos del interesado y cómo ejercerlos.
 - Información respecto al Responsable y/o Encargado del Tratamiento de Datos, así como del Delegado de Protección de Datos en su caso.
- El consentimiento siempre positivo, nunca negativo.
- El consentimiento debe poder revocarse con la misma facilidad.
- Equilibrado en la relación (e.g. empleado-empendedor)
- No será válido usar extensas políticas de privacidad ilegibles o llenas de terminología legal.
- El consentimiento debe ser granular, es decir, que exista una opción de consentimiento para cada finalidad. No obstante, una acción positiva puede valer para varios tratamientos (la misma finalidad). (e.g. basta con un acto positivo general para todas las cookies)

Consentimiento

Tipos de Consentimiento

e.g. Seguir navegando en una web sin aceptar cookies

AEPD “**Guía para Responsables del Tratamiento**” de enero del 2017.

El consentimiento *puede ser inequívoco y otorgarse de forma implícita* cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).

Directrices sobre el Consentimiento del Grupo de Trabajo del art 29

El mero hecho de seguir utilizando la web (scroll down o seguir ojeando la página) no satisface los nuevos requisitos del consentimiento (en el sentido comentado de acción clara y afirmativa).

Y ello porque ese supuesto consentimiento manifestado en “seguir navegando” no se distingue de forma suficientemente clara de la conducta de quien no ha reparado en el banner de cookies, ni ha leído su contenido, y sigue leyendo el texto de la web.

Consentimiento

Cookies

- Las cookies sólo pueden cargarse en el equipo del usuario DESPUÉS (no antes) de que éste otorgue su consentimiento.
- No se puede interpretar como “consentimiento inequívoco” sin más, que el usuario siga navegando por la web.

El GT29 interpreta (advierte) que el mero hecho de seguir utilizando la web (scroll down o seguir ojeando la página) no satisface los nuevos requisitos del consentimiento (en el sentido comentado de acción clara y afirmativa).

- El consentimiento del usuario tiene que ser inequívoco, es decir, activo (“acción afirmativa clara” “específica” e “inequívoca” en la nomenclatura del RGPD).
- De acuerdo con el RGPD, hay que implementar un sistema técnico que nos permita defender (y acreditar en el futuro) que el consentimiento de nuestros usuarios al uso de nuestras cookies (y de terceros) fue inequívoco.

Consentimiento

Cookies

Protección de datos

Cuando visita cualquier website, este debe almacenar la información de su navegador mediante el uso de "cookies".

Esta información nos sirve para conocer sus preferencias, dispositivo desde el que navega (ordenador, tablet o teléfono) y hacer que la web funcione como usted espera.

☒ Obligatorio ☐ Preferencias ☐ Soy mayor de edad

Mostrar
detalles ▼

1/3 Seleccionado

Guardar

Acepto

Consentimiento

Cookies

Protección de datos

Cuando visita cualquier website, este debe almacenar la información de su navegador mediante el uso de "cookies".

Esta información nos sirve para conocer sus preferencias, dispositivo desde el que navega (ordenador, tablet o teléfono) y hacer que la web funcione como usted espera.

☒ Obligatorio ☐ Preferencias ☐ Soy mayor de edad

Ocultar
detalles ^

1/3 Seleccionado

Guardar

Acepto

Obligatorio (1)

Preferencias (2)

<https://armeriavaro/content/2-aviso-legal>

< >

Las cookies necesarias ayudan a hacer que un sitio web sea utilizable al habilitar funciones básicas como la navegación de página y el acceso a áreas seguras del sitio web. La página web no puede funcionar correctamente sin estas cookies.

Nombre	Proveedor	Que hace	Caducado	Permitir (Aceptar todo)
Shopping cart	PrestaShop	This provides, and keeps the product...	30 days	<input checked="" type="checkbox"/> Permitir

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

[Términos y condiciones de uso](#)[Política de privacidad](#)[Política de cookies](#)[Política anti-spam](#)

Política de Cookies

Cookies

Este sitio web [www.acrelianews.com] en adelante sitio web, utiliza una tecnología denominada "cookies" con la finalidad de recabar información sobre el uso del sitio Web.

Las cookies son pequeños dispositivos de almacenamiento y recuperación de datos que se instalan en su equipo informático con las finalidades aquí expresadas; en ningún caso nuestras cookies tratarán datos personales o que comprometan su privacidad.

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

Consentimiento

Con el uso de este sitio web Vd. consiente y está de acuerdo en que alojemos estas cookies en su ordenador o dispositivo para los fines aquí expresados.

Si decide no aceptar nuestras cookies, podrá continuar utilizando nuestro sitio web de la forma habitual, aunque es posible que su experiencia de usuario se vea ligeramente perjudicada.

Tipo de Cookies y Finalidad

A continuación ACRECENTA SOLUTIONS SL expone el tipo de cookies utilizadas en el sitio web, así como su finalidad y en su caso las cookies utilizadas de terceros (proveedor del servicio):

- 1. Cookies de autenticación o identificación de usuario:** Permiten la personalización por parte del usuario.
- 2. Cookies Técnicas:** Mostrar página web, gestión de pedidos, recordar preferencias de usuario.
- 3. Cookies de análisis:** Miden y analizan la navegación de los usuarios, permiten el seguimiento y análisis del comportamiento de los usuarios, la elaboración de perfiles anónimos de navegación de los usuarios e introducir mejoras en función del análisis de los datos de uso que hacen los usuarios

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

4. Cookies de visualización de contenidos de plataformas externas: Estos servicios permiten visualizar contenidos alojados en plataformas externas directamente desde las páginas de esta web e interactuar con estos.

5. Cookies de Interacción con redes sociales y plataformas externas: Estos servicios permiten interactuar con redes sociales u otras plataformas externas directamente desde las páginas de esta web.

Las aplicaciones que utilizamos para obtener información de la navegación, medir y analizar la audiencia son:

Google Analytics: www.google.com/analytics gestionado por Google inc. [Política de privacidad](#)

Google Dobleclick: www.google.com/doubleclick gestionado por Google inc. [Política de privacidad](#)

Yandex metrica: metrica.yandex.com gestionado por Yandex Europe AG [Política de privacidad](#)

Las aplicaciones que utilizamos para visualizar contenidos de plataformas externas son:

Youtube: www.youtube.com gestionado por Google inc. [Política de privacidad](#)

Las aplicaciones que utilizamos para interaccionar con redes sociales y plataformas externas son:

Addthis: www.addthis.com gestionado por Clearspring Technologies Inc. [Política de privacidad](#)

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

Desinstalación de Cookies

Su navegador, en ocasiones, puede generar un mensaje instantáneo que le brindará la posibilidad de oponerse a la instalación de estas cookies. En el supuesto que su navegador no le facilite esta posibilidad de forma automática, Vd. podrá inhibir la instalación de las mismas siguiendo las instrucciones de su navegador.

Para permitir, conocer, bloquear o eliminar las cookies instaladas en su equipo puede hacerlo mediante la configuración de las opciones del navegador instalado en su ordenador.

Vd. puede encontrar información sobre cómo hacerlo en las siguientes direcciones:

Firefox desde <https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias?redirectlocale=es&redirectslug=habilitar-y-deshabilitar-cookies-que-los-sitios-we>

Chrome desde <https://support.google.com/chrome/answer/95647?hl=es>

Explorer desde <https://support.microsoft.com/es-es/help/17442/windows-internet-explorer-delete-manage-cookies>

Safari desde https://support.apple.com/kb/PH19214?viewlocale=es_ES&locale=es_ES

Opera desde <http://help.opera.com/Windows/11.50/es-ES/cookies.html>

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

Cambios en la Política de Cookies

En cualquier momento ACRECENTA SOLUTIONS SL puede modificar la política de cookies por lo que le rogamos que consulte de manera periódica la misma ya que se pueden producir cambios.

Contacto

Si Vd. utiliza otro navegador, puede obtener más información sobre cómo configurar la instalación de las cookies a través de la sección de ayuda o asistencia de dicho navegador. Si necesita ayuda para llevar a cabo la configuración de las cookies con su navegador, por favor, envíenos un e-mail a cookies@acrecenta.com y nos pondremos en contacto con Vd. lo antes posible con la información necesaria.

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

[Términos y condiciones de uso](#)[Política de privacidad](#)[Política de cookies](#)[Política anti-spam](#)

Política de Privacidad

Versión publicada el 3 de mayo de 2018.

1.-

En cumplimiento de la Ley española 15/99 de 13 de diciembre de protección de datos de carácter personal (LOPD), y del 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 (RGPD), le informamos que todos los datos de carácter personal que nos facilite a través del sitio web acrelia.news formarán parte de un tratamiento titularidad de ACRECENTA SOLUTIONS SL (en adelante, ACRECENTA), titular del citado sitio web y con domicilio social en avenida Martí Pujol 280, local 2 08911 Badalona (Barcelona) y NIF B66656281, cuya finalidad es la de prestar los servicios solicitados e informarle sobre los productos y servicios de ACRECENTA.

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

[Términos y condiciones de uso](#)[Política de privacidad](#)[Política de cookies](#)[Política anti-spam](#)

Política anti-spam

Como proveedor de servicios de e-mail marketing es nuestra obligación conseguir que nuestros usuarios cumplan las normativas sobre comunicaciones comerciales.

Acrelia news [te ayuda a seguir las mejores prácticas](#) a la hora de comunicarte con tus suscriptores y conseguir nuevos contactos, pero es necesario que conozcas y apliques la normativa vigente en tu país sobre protección de datos y servicios de la sociedad de la información y comercio electrónico.

Cómo enviar comunicaciones comerciales

En Europa para remitir comunicaciones comerciales es necesario cumplir con los requisitos que exponemos a continuación:

Consentimiento

Cookies

Utilizamos cookies propias y de terceros para mejorar nuestros servicios mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. [OK](#) [Leer más](#)

[Términos y condiciones de uso](#)[Política de privacidad](#)[Política de cookies](#)[Política anti-spam](#)

Términos y condiciones de uso y contratación de Acrelia News

Versión publicada el 3 de mayo de 2018.

1. TITULARIDAD DEL SITIO WEB

1.1. El titular del sitio web www.acrelianews.com es la compañía ACRECENTA SOLUTIONS SL (en adelante, ACRECENTA) inscrita en el registro

Consentimiento

Cookies

Política de Cookies

El Corte Inglés utilizamos cookies con el objetivo de prestar un mejor servicio y proporcionarte una mejor experiencia en tu navegación. Queremos informarte de manera clara y precisa sobre las cookies que utilizamos, detallando a continuación, qué es una cookie, para qué sirve, qué tipos de cookies utilizamos, cuáles son su finalidad y cómo puedes configurarlas o deshabilitarlas si así lo deseas.

Consentimiento

En El Corte Inglés nunca guardamos los datos personales de nuestros usuarios, a excepción de la dirección IP de acuerdo a lo descrito anteriormente, salvo que quieras registrarte, de forma voluntaria con el fin de realizar compras de los productos y servicios que ponemos a tu disposición o de recibir información sobre promociones y contenidos de tu interés. Al navegar y continuar en nuestra web nos indicas que estás consintiendo el uso de las cookies antes enunciadas, y en las condiciones contenidas en la presente Política de Cookies.

El Corte Inglés. Todos los derechos reservados.

Relación de cookies utilizadas en el dominio elcorteingles.es

NOMBRE	SERVIDOR DE ENVÍO	FINALIDAD	PROPIA / TERCEROS	EXCLUIDA / NO EXCLUIDA DEL DESEMPEÑO DE LA INFORMACIÓN Y CONSENTIMIENTO
ASPSESSIONID	www.elcorteingles.es	Estrictamente Necesaria	Propia	Sí
ASPSESSIONIDQQAS QQTR	www.elcorteingles.es	Estrictamente Necesaria	Propia	Sí
DYN_USER_CONFIG.M	www.elcorteingles.es	Estrictamente Necesaria	Propia	Sí
DYN_USER_ID	www.elcorteingles.es	Estrictamente Necesaria	Propia	Sí
ECI	www.elcorteingles.es - www3.elcorteingles.es	Estrictamente Necesaria	Propia	Sí
ECISA	www.elcorteingles.es	Estrictamente Necesaria	Propia	Sí

https://www.elcorteingles.es/sgfm/SGFM/contents/documents/gdpr/es_ES/politica_de_cookies.pdf

Roles

Roles

DIFERENCIAS ENTRE DPO, RESPONSABLE DEL TRATAMIENTO, ENCARGADO DEL TRATAMIENTO Y RESPONSABLE DE PRIVACIDAD

RESPONSABLE DEL TRATAMIENTO	ENCARGADO DEL TRATAMIENTO	DPO	RESPONSABLE DE PRIVACIDAD
<ul style="list-style-type: none">✓ Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que en el ejercicio de su actividad trata con datos personales.✓ Por ley, tiene la obligación de determinar cómo se tratan y gestionan los datos personales en su entidad, haciéndose responsable de la creación y gestión de los ficheros.	<ul style="list-style-type: none">✓ Persona física o jurídica, autoridad pública, servicio u otro organismo que en el ejercicio de su actividad trata datos de carácter personal que son responsabilidad del Responsable del Tratamiento.	<ul style="list-style-type: none">✓ Ayuda al Responsable o al Encargado del Tratamiento. Es un profesional con conocimientos especializados de la normativa y la práctica en materia de protección de datos.✓ Los DPO pueden ser empleados o no del Responsable del Tratamiento, pero deben estar en condiciones de desempeñar sus funciones de manera independiente.	<ul style="list-style-type: none">✓ Persona que trabaja en la empresa y que, además de su cargo, también es designada para coordinar todos los aspectos relacionados con la adecuación de las actuaciones de la entidad en materia de protección de datos.
EJEMPLO: ✓ EMPRESA, S.A.	EJEMPLO: ✓ ORDENADORES, S.A. (Empresa que se encarga del mantenimiento del sistema informático de EMPRESA, S.A.)	EJEMPLO: ✓ CONVERSIA (Empresa que presta su servicio de adaptación de protección de datos a EMPRESA, S.A.)	EJEMPLO: ✓ David Cuesta (Empleado de EMPRESA, S.A.)

* **CORRESPONSABLES DEL TRATAMIENTO:** Cuando dos o más Responsables del Tratamiento determinan conjuntamente la finalidad, contenido y uso del tratamiento de datos, mediante un acuerdo por escrito que delimita sus responsabilidades, éstos se convierten en corresponsables del tratamiento.

EJEMPLO:

✓ EMPRESA, S.A. y ENTIDAD, S.A. (Ambas son empresas del GRUPO EMPRESARIAL y comparten bases de datos personales).

Roles

El Responsable del Tratamiento

Persona física y/o jurídica, privada o pública, que decide sobre el tratamiento de los datos. Su condición de Responsable hace que esté sujeto a los requerimientos establecidos en la normativa y que, en consecuencia, tenga que observar cuantas obligaciones disponga el Reglamento General de Protección de Datos.

Roles

El Encargado del Tratamiento

Persona física y/o jurídica, privada o pública, que trata datos personales por cuenta del responsable del tratamiento. Suele ser un tercero externo a la empresa. Hablaríamos, por ejemplo, de asesorías laborales, mutuas de prevención de riesgos, etc.

Roles

RESPONSABLE Y ENCARGADO

Responsable del tratamiento	Encargado del tratamiento
Decide sobre el tratamiento de datos personales.	No decide. Trata datos personales por cuenta del responsable.
Da instrucciones al encargado.	Tiene que seguir las instrucciones del responsable.

Empresa que presta servicios a la asociación, tales como almacenamiento de bases de datos, contador externo, asistencia técnica, etc.

Roles

¿Cómo se regula la relación entre el responsable y el encargado?

Con un contrato por escrito en el que conste que el encargado del tratamiento cumplirá con lo siguiente:

- Únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- No aplicará ni utilizará los datos con un fin distinto al que figure en el contrato.
- No comunicará los datos, ni siquiera para su conservación, a otras personas.
- Expondrá qué hará con los datos una vez finalizado el servicio correspondiente.
- Deben recogerse las medidas de seguridad que el encargado del tratamiento está obligado a seguir.

Datos Especialmente protegidos

Datos Especialmente protegidos

Los datos especialmente protegidos o datos sensibles son aquellos que debido a su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona, es necesaria una mayor protección que el resto de datos personales, y que de manera general sólo con el consentimiento expreso y por escrito del afectado pueden ser objeto de tratamiento.

Datos Especialmente protegidos

Listado

LOPD 1999

- Ideología
- Afiliación sindical
- Religión
- Creencias
- Origen racial o étnico
- Salud
- Vida sexual

RGPD

- Opiniones políticas
- Afiliación sindical
- Convicciones religiosas
- Convicciones filosóficas
- Origen racial o étnico
- Datos relativos a la salud
- Vida sexual
- Dato genético
- Dato biométrico
- Orientación sexual



Datos Especialmente protegidos

Medidas Obligatorias

RGPD

Registro de las Actividades de Tratamiento

Hay que realizar y mantener actualizado un registro de todos los tratamientos que se realicen, documentándolos y aportando una serie de información específica.

Evaluación del Impacto en la Protección de Datos

Si se trata o se prevé tratar a gran escala esta categoría especial de datos se ha que realizar un EIPD (análisis del riesgo que puede entrañar el tratamiento de dichos datos personales para los derechos y libertades de los afectados).

Datos Especialmente protegidos

Medidas Obligatorias

RGPD

Medidas de Seguridad

- **Cifrado** de los datos en su comunicación y almacenamiento
- **Registro de accesos**, con fecha y personal que accedió
- Elaboración de una **lista de personas autorizadas**
- Establecer un **procedimiento** seguro para su tratamiento

Acceso a datos por cuenta de terceros

Acceso a datos por cuenta de terceros

Se produce un acceso a datos por cuenta de terceros:

- Cuando una entidad (tercero) accede a datos de otra que le ha encargado un servicio.

Servicios informáticos

Buckups online

Gestoría laboral

Prevención de riesgos laborales

Servicio de limpieza del edificio

Servicio de mantenimiento del edificio

Seguridad del edificio

Acceso a datos por cuenta de terceros

Se registrá por:

- La relación establecida entre el **Responsable del Tratamiento** (de la empresa que realiza el encargo y titular de los datos) y el **Encargado del Tratamiento** (de la empresa que recibe el encargo y realizará el acceso).
- Deberá formalizarse y establecerse mediante un **contrato** a tal efecto.

Transferencias Internacionales

Transferencias Internacionales

“Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)”

“Los responsables y encargados del tratamiento podrán realizar transferencias internacionales de datos sin necesidad de una autorización de la Agencia Española de Protección de Datos siempre que el tratamiento de datos observe lo dispuesto en el RGPD y se den una serie de supuestos.”

Transferencias Internacionales

Transferencias internacionales de datos basadas en una decisión de adecuación (artículo 45 RGPD): que los destinatarios de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que haya sido declarado de nivel de protección adecuado por la comisión europea.

Países y territorios están declarados como adecuados (verificar actualización):

- Suiza.
- Canadá.
- Argentina.
- Guernsey.
- Isla de Man.
- Jersey.
- Islas Feroe
- Andorra.
- Israel.
- Uruguay.
- Nueva Zelanda.
- **Estados Unidos:** aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.
- El Escudo de Privacidad ofrece una serie de derechos y obliga a las empresas a proteger los datos personales de modo acorde con los "Principios de privacidad".
- Web de entidades certificadas
[Https://www.privacyshield.gov/list](https://www.privacyshield.gov/list)

Registro de Actividades

Registro de Actividades

¿Qué es?

Los responsables y encargados del tratamiento de datos personales deberán mantener un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

¿Quién está obligado?

- La empresa u organización tenga más de 250 empleados.
- Cuando se realicen tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados, no sean ocasionales, o incluyan categorías especiales de datos personales.
- Se realice un tratamiento de datos personales relativos a condenas e infracciones penales.

Importante: en la práctica todos los tratamientos pueden suponer un riesgo para los derechos y libertades de los interesados, aunque sea ocasional → la mayoría de los responsables o encargados del tratamiento que empleen a menos de 250 trabajadoras estarán obligadas a llevar un registro de actividades de tratamiento.

Seguridad

Seguridad

Los responsables y encargados establecerán las medidas de seguridad técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

Así, se deberán aplicar medidas técnicas y organizativas de acuerdo con:

- a) El coste de la técnica.
- b) Los costes de aplicación.
- c) La naturaleza, el alcance, el contexto y los fines del tratamiento.
- d) Los riesgos para los derechos y libertades.

Seguridad

Medidas organizativas

- **Concienciación**
- **Sensibilización**
- **Formación**

+

- **Políticas**
- **Procedimientos**



- Seudonimización.
- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia.
- Capacidad para restaurar la disponibilidad.
- Capacidad para restaurar la continuidad.
- Proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

Seguridad

Medidas técnicas

- Antispam
- Filtrado de accesos web
- Gestión de parches
- Copias de seguridad
- Cifrado de ficheros
- Cifrado de discos
- Cifrado de USB
- Cifrado de comunicaciones
- VPNs
- Cortafuegos
- **etcétera**



Seguridad

Una primera aproximación

El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD no seguirá siendo válido de forma automática tras la fecha de aplicación del RGPD.

- En algunos casos los responsables podrán seguir aplicando las mismas medidas que establece el Reglamento de la LOPD si los resultados del análisis de riesgos previo se concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado.
- En otras ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas

Seguridad

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	<ul style="list-style-type: none"> - Ambito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos. 	<ul style="list-style-type: none"> - Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes. 	
PERSONAL	<ul style="list-style-type: none"> - Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento. 		
INCIDENCIAS	<ul style="list-style-type: none"> - Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados. 	<ul style="list-style-type: none"> - Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación. 	
IDENTIFICACIÓN Y AUTENTICACIÓN	<ul style="list-style-type: none"> - Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligible de contraseñas activas. 	<ul style="list-style-type: none"> - Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Límite de intentos reiterados de acceso no autorizado. 	

Seguridad

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
CONTROL DE ACCESO	<ul style="list-style-type: none"> - Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. 	<ul style="list-style-type: none"> - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. 	
GESTIÓN DE SOPORTES	<ul style="list-style-type: none"> - Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero. 	<ul style="list-style-type: none"> - Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento. 	<ul style="list-style-type: none"> - Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	<ul style="list-style-type: none"> - Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal. 		<ul style="list-style-type: none"> - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPONSABLE		<ul style="list-style-type: none"> - Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero. 	

Seguridad

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
PRUEBAS		<ul style="list-style-type: none"> - Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado. 	
AUDITORIA		<ul style="list-style-type: none"> - Al menos cada dos años, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero, - Adopción de las medidas correctoras adecuadas. 	
REGISTRO DE ACCESOS			<ul style="list-style-type: none"> - Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TRANSMISIONES			<ul style="list-style-type: none"> - Transmisión de datos cifrada.

Seguridad

La aproximación adecuada

Análisis de Riesgos

+

Evaluación de Impacto



Análisis de Riesgos

Análisis de Riesgos

Los **responsable y encargados** deben llevar a cabo una valoración del riesgo de sus tratamientos realicen, con el fin de **determinar qué medidas aplicar y cómo** hacerlo. Este análisis del riesgo variará en función de:

- a) Los tipos de tratamiento.
- b) La naturaleza de los datos.
- c) El número de interesados afectados.
- d) La cantidad y variedad de tratamientos que realice una misma organización.

Evaluación de Impacto

Evaluación de Impacto

Permite **evaluar de manera anticipada** cuáles son los potenciales **riesgos** a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo "antes del tratamiento" en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados.

Quiebra de Seguridad

Quiebra de Seguridad

Todo **incidente** 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.



Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como la norma establece.

Sanciones

Sanciones

Norma aplicable	Sanciones		
	Leve	Grave	Muy grave
LOPD/RLOPD	900€ - 40.000€	40.001€ - 300.000€	300.001€ - 600.000€
RGPD	No se establece un rango mínimo de cuantía	Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.	Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.