Protección de datos de carácter personal (I)

[2.1] ¿Cómo estudiar este tema?

[2.2] El derecho fundamental de protección de datos

[2.3] El Reglamento europeo de la protección de datos: ámbitos de aplicación

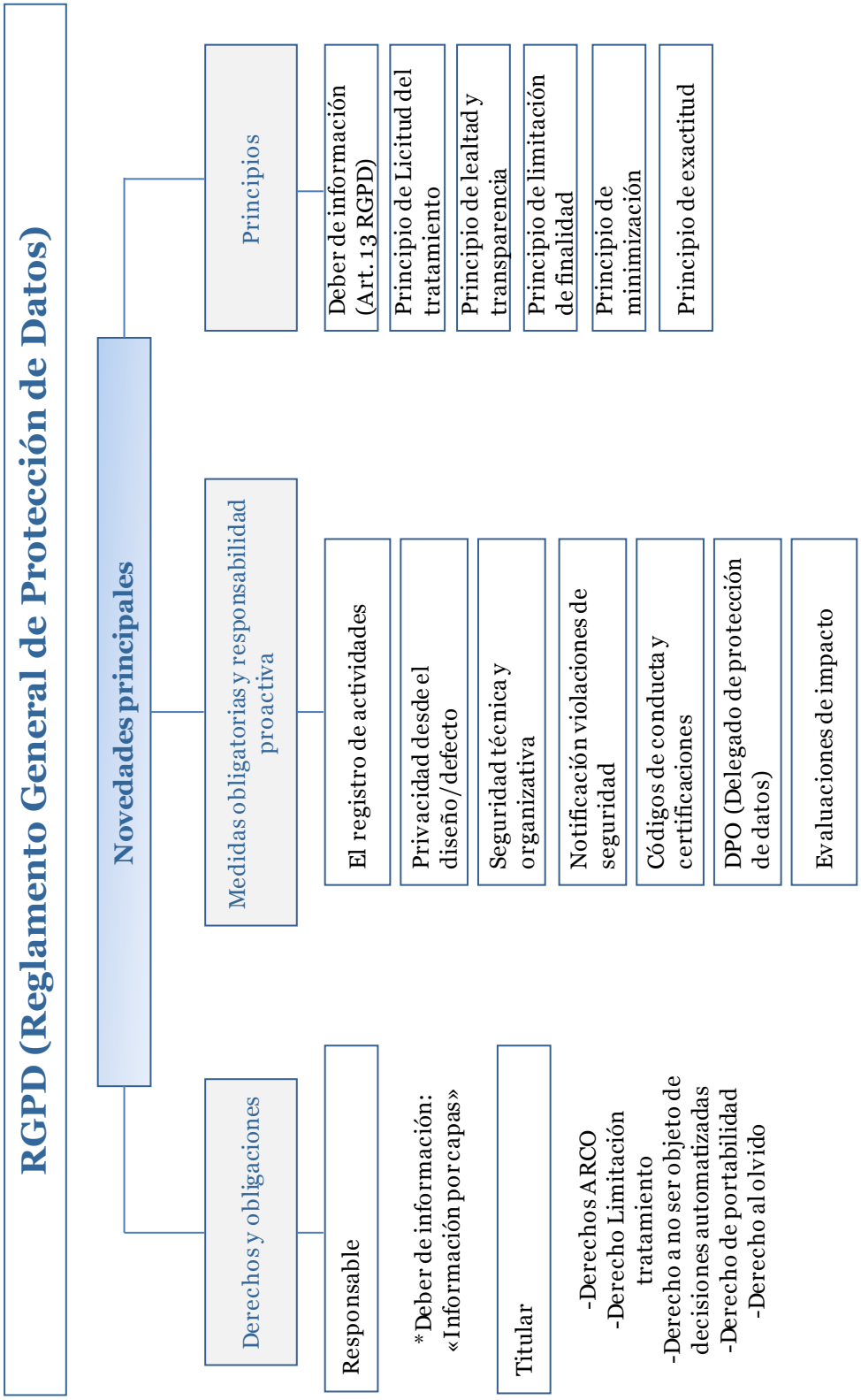
[2.4] Principios principales del RGPD

[2.5] Algunas definiciones de interés del RGPD

[2.6] Las transferencias internacionales. *Cloud computing* y *apps*

TEMA 2

Esquema



Ideas clave

2.1. ¿Cómo estudiar este tema?

Para estudiar este tema deberás leer y comprender las **Ideas clave** expuestas en este documento.

En este tema realizaremos una introducción al derecho a la protección de datos de carácter personal y su regulación:

- Analizar el **derecho fundamental** a la protección de datos y su regulación a nivel nacional e internacional.
- Comprender la posición jurídica y obligaciones del responsable y encargado de tratamiento.
- Estudiar los principios generales del Reglamento europeo de protección de datos y su afección en la normativa nacional.
- Entender las principales definiciones del Reglamento europeo de protección de datos aplicadas al sector de la informática.
- Repasaremos qué son las transferencias internacionales y su implicación con el nuevo Reglamento europeo de protección de datos.

2.2. El derecho fundamental de protección de datos

El **artículo 8 de la Carta Europea de Derechos Humanos** reconoce el derecho fundamental a la protección de datos. Más adelante, el derecho de protección de datos se elevó a categoría de **derecho fundamental autónomo**, independiente del derecho a la intimidad, lo que quedó demostrado el hecho de que la propia Carta reconociese el **derecho a la intimidad personal y familiar** en un artículo distinto; el artículo 7.

En el **artículo 16 del TFUE** (Tratado de Funcionamiento de la Unión Europea) reconoció este derecho afirmando que: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan».

Respecto a la jurisprudencia y mención de este derecho, hay dos pronunciamientos altamente significativos; las SSTC 254/1993 y 292/2000:

- En la primera de ellas, la **STC 254/1993**:
  - Se define por primera vez lo que entonces se denominó «**libertad informática**».
  - El recurso de amparo que dio lugar al pronunciamiento tuvo su origen en la petición de información por parte de un ciudadano vasco al Gobernador Civil de Guipúzcoa sobre la existencia de **ficheros automatizados de la Administración del Estado** que pudiesen contener datos relativos a su persona.
  - Se solicitaba también, en caso de que estos existieran, la indicación del **organismo estatal** en el que se encontraban, la **finalidad** de los ficheros, la autoridad que los controlase y su residencia habitual y, además, se pedía la comunicación de los datos existentes que le afectasen, de forma inteligible y sin demora.
  - La solicitud fue **denegada por la Administración** y, agotada la vía administrativa, la denegación fue confirmada por las sucesivas instancias judiciales, interponiéndose finalmente recurso de amparo al Tribunal Constitucional.
  - El TC subraya la importancia que posee la satisfacción de estos derechos, tomando como referencia el **artículo 18 C.E.**

- Respecto a la **sentencia 292/2000:**
  - Se reafirma la importancia de las cuestiones relacionadas con la **protección jurídica de los datos personales,** consolidando de modo definitivo la consideración de la misma como un **derecho fundamental**.
  - Concibe el derecho fundamental a la protección de datos como un **derecho netamenteprestacional** del que dimanan derechos del afectado—que operan como paralelas obligaciones del responsable—junto con específicas **obligaciones**para este último.
  - El art. 18.4 CE tendrá plena autonomía respecto al derecho de intimidad (art. 18.1 CE). Es importante diferenciar:

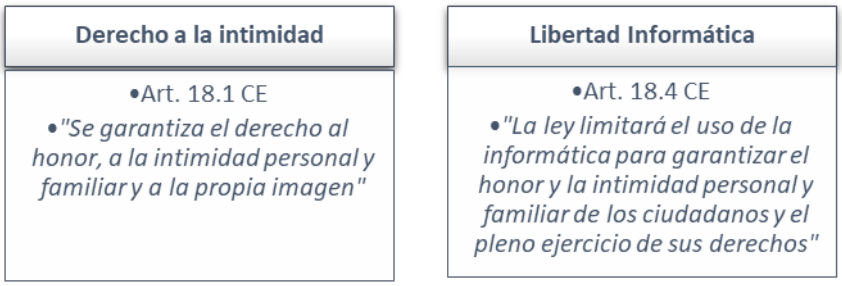


Figura 1. Derecho a la intimidad y Libertad a la informática.

La llamada **libertad informática** es el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

El derecho fundamental de protección de datos: De la antigua Directiva al Reglamento europeo actual

La antigua Directiva 95/46/CE es previa a la Carta y al TFUE, por lo que no pudo reflejar lo contenido en estos dos último, pero sí que tuvo en cuenta el **Convenio Europeo de Derechos Humanos y el Convenio 108**. La Directiva pretende que los tratamientos de datos no violen los derechos fundamentales y en particular el derecho a la intimidad y así lo establece en el considerando 2.

El Reglamento ya no solo considera que los tratamientos de datos personales pueden violar los derechos fundamentales de las personas (en particular, el derecho a la intimidad) sino que parte de la base de que el simple hecho de tratar datos personales puede violar el propio **derecho a la protección de datos de carácter personal**. En definitiva, el Reglamento europeo tiene como uno de sus objetos principales la regulación del derecho fundamental a la protección de datos de carácter personal reconocido en el artículo 8 de la Carta Europea de Derechos Humanos.

El Reglamento en el considerando 7 afirma que «las personas físicas deben tener el **control de sus propios datos personales**». El control al que se refiere el legislador es la piedra angular del derecho, el que reconoce sus principios y los derechos de los afectados, tal y como se reflejan en el artículo 12 y 13 del Reglamento Europeo.

2.3. El reglamento europeo de protección de datos: ámbito de aplicación

El estudio del ámbito de la aplicación de una disposición es uno de los análisis esenciales que debe realizarse de forma previa a cualquier otro acto de interpretación de la norma.

Ámbito de aplicación material

El Reglamento europeo establece que es de aplicación a los tratamientos total o parcialmente automatizados y a los tratamientos no automatizados de datos personales que se contengan o en un futuro vayan a ser incluidos en un fichero.

NO son de aplicación:

- Las actividades **fuera del ámbito de aplicación del Derecho de la Unión.** La excepción afectaría meramente a los tratamientos de datos que fuesen necesarios para el desarrollo de estas actividades. Ej. Actividades relativas a la seguridad nacional.
- Las actividades de **política exterior y de seguridad común** realizadas por los Estados miembros (PESC). El objetivo de PESC es mantener la paz y reforzar la seguridad.
- Las actividades **personales o domésticas**.

Estos tratamientos no tienen que tener ninguna conexión profesional o comercial o interés oneroso.

Es de mencionar el **Dictamen 5/2009 del GT29** donde se especifican excepciones concretas domésticas.

Accede a más información del Dictamen 5/2009 del GT29 https://www.apda.ad/system/files/wp163_es.pdf

Ejemplo: La exención se aplica a las personas físicas que tuviesen en su móvil un listado de contactos.

- Las actividades de persecución de **infracciones penales.**
  - Los Estados pueden limitar los tratamientos a entidades privadas e imponer obligaciones y derechos siempre que dicha limitación sea una medida proporcional y necesaria en una sociedad democrática.
  - Pensemos en los tratamientos de datos necesarios para la expedición de DNI, en los tratamientos de datos realizados por la policía científica o de ciberataques.

Ámbito de aplicación territorial

El objetivo del Reglamento, a diferencia de la Directiva que trataba *armonizar* la protección de las normas estatales de protección de datos, es establecer un **nivel de protección «equivalente en todos los Estados miembros»** y garantizar una aplicación de estas normas «coherente y homogénea»

A partir de ahora, las sociedades establecidas fuera de la UE pero que actúan en su territorio tendrán que aplicar las mismas reglas cuando ofrezcan bienes y servicios en el mercado comunitario.

El Reglamento contempla tres escenarios para su aplicación:

A. En el contexto de las actividades de **un establecimiento del responsable o del encargado en la Unión** (Art. 3.1) independientemente de que dicho tratamiento tenga lugar en la Unión o no. (El concepto 'establecimiento' se extiende a cualquier actividad real y efectiva aún mínima ejercida mediante una instalación estable. Ej. Google España).

B. Cuando el responsable no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del **Derecho internacional público.**

C. Cuando responsable o encargado del tratamiento **no esté establecido en la Unión.** Para que se apliquen las normas europeas es necesario:
   - Los **datos personales sean de residentes en la Unión**.
   - Las actividades del tratamiento se refieran a un **objeto determinado** que puede ser:
     - La oferta de bienes o servicios a dichos interesados. Ej. La página web, el idioma o moneda.
     - La observación del comportamiento de dichos interesados en la medida que este comportamiento tenga lugar en la Unión.

» **Caso *Google Spain* (TJUE 13 mayo 2014**). Era la primera ocasión en la que se solicita al TJUE que se interpretara en la antigua Directiva en relación con los motores de búsqueda de Internet respondiendo a los cambios propiciados por el desarrollo tecnológico. La Audiencia Nacional planteó cuestión prejudicial al TJUE preguntando cuáles eran las obligaciones que tenían los gestores de motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contienen sus datos personales y permite relacionarles con la misma, sea localizada, indexada y puesta a disposición de los internautas de forma indefinida.(Google disponía de un establecimiento en un Estado miembro europeo (España).

  El Tribunal de Justicia sostiene que procede considerar que **el tratamiento de datos personales** realizado estaba **«indisociablemente ligado al establecimiento creado por esta misma empresa en España»** aun cuando este último no realice el tratamiento de datos personal o actividad directamente relacionada con el mismo, pues se trata de actividades de publicidad de la empresa. Sin publicidad, Google no podría ofertar sus servicios de motor de búsqueda.

2.4. Principios principales del RGPD

La gran mayoría de los principios de la antigua Directiva se contemplan en el Reglamento, no obstante, el Reglamento introduce un **nuevo modelo de protección de datos** para Europa. Podemos decir que el modelo pasa de la **gestión de los datos al uso responsable de la información** que se aprecia en cuestiones como el principio de responsabilidad proactiva, los principios de privacidad desde el diseño y por defecto, la figura del DPO, el fortalecimiento de los códigos de conducta, la

exigencia de llevar el registro de actividades del tratamiento, la regulación de las medidas de seguridad, etc. Se incrementa la idea de la **responsabilidad proactiva** y el ámbito de la **autorregulación**, al mismo tiempo que se fortalece el aspecto institucional, a nivel nacional y de la Unión Europea.

Las reglas del juego son **más uniformes** a nivel de la Unión Europea, pero al mismo tiempo se deja mayor margen de apreciación y valoración a los responsables y encargados. Ya no basta con inscribir los ficheros (obligación que desaparece) o adoptar el documento de seguridad, implementar las medidas y redactar clausulas. A partir de ahora, será necesario adoptar **decisiones propias en función de los tratamientos de datos** que se llevan a cabo y la de la naturaleza de estos. Esto estará mucho más al alcance de las grandes compañías y AAPP que de las pymes y pequeños organismos públicos.
Desarrollemos a continuación los principios:

Principio de la licitud del tratamiento

La antigua LOPD ya prohibía expresamente la recogida de datos por medios fraudulentos, desleales o ilícitos. Ahora, el RGPD establece de manera expresa que los datos personales deben ser tratados de manera lícita, leal y transparente.

Principio de la lealtad y transparencia

La información debe ser **accesible** y el **lenguaje sencillo.** El Reglamento europeo se declara expresamente en contra de las cláusulas informativas extensas y prolijas.

Se apuesta claramente por la **información por capas** y por la web como un soporte universal para las entidades, además de consolidar los planteamientos previos desarrollados para las *cookies*. En tal sentido, el soporte web está llamado a ser un soporte imprescindible en la información vinculada a las captaciones de datos con tecnologías como Internet de las Cosas o *wearables*.

Para facilitar el cumplimiento de este derecho de información por capas, la AEPD, en colaboración con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, ha publicado la Guía para el cumplimiento del deber de informar.

Se deberá informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Se exigirá mayor precisión y detalle en la información, simplificación en las formas y contenidos, una estrategia multicapa en los soportes y canales.

Principio de limitación de la finalidad

El derecho a la limitación puede ejercerse cuando se cumpla alguna de las condiciones siguientes:

- El titular impugne la exactitud de los datos personales.
- Cuando el tratamiento es ilícito y el titular se opone a la supresión y solicita la limitación de su uso;
- Cuando el titular sí necesite los datos personales para su interés, aunque no lo necesite el responsable.
- El titular se opone al tratamiento en virtud del art. 21.1 hasta que se compruebe si los motivos legítimos del responsable están por encima de los del titular.

Principio de minimización de datos

El principio de minimización de datos se refiere expresamente:

- A la cantidad de datos recogidos (debe ser limitada).
- Al perímetro del tratamiento.
- Al período de tiempo de retención.
- Al número de personas con acceso a los mismos.

En concreto, el legislador establece que el responsable deberá aplicar las medidas (técnicas y organizativas apropiadas) para poder garantizar que solo sean objeto de tratamiento los datos personales necesarios refiriéndose a la extensión de dicho tratamiento, al plazo de conservación y a la accesibilidad.

Principio de exactitud.

Los datos personales deber ser **exactos** y dado el caso, deberán ser actualizados, para ello, se deberán adoptar 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.

2.5. Algunas definiciones de interés del RGPD

Dato personal

Es toda **información sobre una persona física identificada o identificable** (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador.

Por ejemplo, son datos personales:

- Un nombre.
- Un número de identificación.
- Datos de localización o un identificador en línea).
- O mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas.

El IP del ordenador, nuestro DNI, nuestro ADN, nuestra huella dactilar, la forma de caminar o la forma de escribir en el teclado son datos personales.

También existen los denominados datos **especialmente protegidos**, en los que además de los datos de salud, se encuentran los que hagan referencia a tu ideología, religión, origen racial, vida sexual, y comisión de infracciones penales y administrativas

Tratamiento de datos

Se trata de:

- Cualquier **operación o conjunto de operaciones** realizadas sobre datos personales o conjuntos de datos personales.
- Ya sea por procedimientos automatizados o no.
- Como, por ejemplo, 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.

Elaboración de perfiles

Se trata:

- De todo tratamiento **automatizado** de datos personales.
- Que se utiliza para evaluar o analizar aspectos «personales».
- En concreto, para predecir cuestiones relacionadas con:
  - Rendimiento profesional.
  - Situación económica.
  - Salud, preferencias personales.
  - Intereses, fiabilidad.
  - Comportamiento.
  - Ubicación.
  - Movimientos de dicha persona física.

Fichero

Podemos decir en términos generales que se trata de todo conjunto **«estructurado»** de datos personales.

Normas corporativas vinculantes *(Corporate Binding Rules)*

Se tratan de:

- **Políticas** de protección de datos personales.
- Asumidas por un responsable o encargado en la UE
- Para **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.

Fuentes accesibles al públic

Se tratan de:

- **Ficheros** cuya consulta puede ser realizada por **cualquier persona**, no impedida por una norma limitativa o sin más exigencia que el abono de una contraprestación.

- **Exclusivamente:**
  - Repertorios telefónicos.
  - Listas de grupos profesionales (nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo), podrá incluir domicilio postal completo, número telefónico, número de fax y dirección electrónica, número de colegiado, fecha de incorporación y situación de ejercicio profesional.
  - Diarios y boletines oficiales.
  - Censo promoción: base de datos personales (nombres apellidos y domicilios) de los ciudadanos que constan registrados obligatoriamente en el censo electoral.
  - Medios de comunicación. Internet NO es, a los efectos de protección de datos, un medio de comunicación social, sino un canal de comunicación, por lo que no se considera que es una fuente accesible al público.

Datos biométricos

Se tratan de:

- Datos personales.
- Obtenidos a partir de un **tratamiento técnico** específico.
- Relativos a las características **físicas, fisiológicas o conductuales** de una persona física.
- Que permitan o confirmen la identificación única de dicha persona.
- Como imágenes faciales o datos dactiloscópicos.

Por ejemplo, las huellas dactilares o el iris de los ojos.

Datos genéticos

Se tratan de:

- Datos personales.
- Relativos a las características **genéticas** heredadas o adquiridas de una persona física.
- Que proporcionen una información única sobre la fisiología o la salud de esa persona.
- Obtenidos en particular del análisis de una **muestra biológica** de tal persona.

Dirección IP

La AEPD ha considerado en sus Informes Jurídicos 327/2003 y en el de 1 de marzo de 2007, que la dirección IP y el nombre de usuario deben ser entendidos como datos de carácter personal.

Las claves identificativas IP no concretan a la persona del usuario, sino solo el ordenador usado, por lo que para poder conocer el número de teléfono y titular del contrato se requiere posterior autorización judicial.

Correo electrónico

Se pueden darse dos supuestos, en atención al grado de identificación del mismo con el titular de la cuenta de correo:

- Email con información de su titular (nombre y apellidos, empresa, país) «Josegarcia@abalca.com». Identifica al titular cuenta.
- Email con denominación abstracta. No muestra datos relacionados con el titular de la cuenta. «red104@pod.org».

Datos disociados (Art. 5.1.e)

Se tratan de los datos que no permiten la identificación de un afectado o interesado.

Anonimización

Destacar en este punto la importancia de la Guía de la AEPD.

Seudonimización (Art. 4.5)

Se trata de:

- Un tratamiento de datos personales.
- Donde **NO pueden atribuirse a un interesado sin utilizar información adicional**.

- Siempre que dicha información adicional 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.

Responsable del tratamiento

Se trata de:

- La persona física o jurídica, autoridad pública, servicio u otro organismo.
- Que solo o junto con otros, **determine los fines y medios del tratamiento.**

Encargado del tratamiento.

Se trata de:

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

Según el RGPD:

- No recurrirá a otro encargado sin la autorización por escrito, específica o general, del responsable.
- El tratamiento se regirá por un contrato con el responsable (objeto, duración, finalidad del tratamiento, tipo de datos y categorías de interesados, obligaciones y derechos del responsable) u otro acto jurídico por ejemplo: resolución administrativa.
- Comisión podrá fijar cláusulas contractuales tipo.
- Contrato por escrito y formato electrónico.
- Tratará los datos siguiendo instrucciones del responsable.
- Garantizará confidencialidad, personas autorizadas para tratamiento.
- Tomará las medidas necesarias en materia de seguridad.
- Cuando recurra a otro encargado, dispondrá de contrato con las mismas obligaciones estipuladas en el contrato con el responsable. Por escrito y formato electrónico.
- Seguirá siendo responsable ante el responsable.
- Asistirá al responsable, con medidas técnicas y organizativas.
- Ayudará al responsable a garantizar el cumplimiento de la seguridad, notificar violación a la autoridad de control e interesado.

- Suprimirá o devolverá todos los datos al finalizar servicio, y suprimirá las copias salvo que se requiera su conservación.
- Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones. Inspecciones, auditorias.
- Si infringe el RGPD al determinar los fines y medios del tratamiento, será considerado responsable.

2.6. Las transferencias internacionales. *Cloud computing* y *apps*.

Una transferencia internacional de datos es un tratamiento de datos que supone una transmisión de los mismos **fuera del territorio de la UE**, ya sea una cesión de datos o un supuesto de encargado del tratamiento.

El **exportador de datos** es la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero. El **importador de datos** es la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargado del tratamiento o tercero.

Se podrán hacer transferencias internacionales solo si se cumple el Reglamento europeo.

Solo se podrán transmitir datos a aquellos países, territorios, sectores u organismos internacionales respecto de los que la Comisión Europea haya considerado que; disponen de un **nivel adecuado de protección** o, se aporten **garantías suficientes** o, se den algunas de las **circunstancias previstas como excepciones**, y siempre y cuando se observen los demás requisitos del mencionado RGPD. Hasta la fecha la **Comisión Europea** ha considerado países que ofrecen un **nivel adecuado** de protección a los siguientes países y territorios:

- Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda.

- Canadá (solo cuando a la entidad destinataria le sea de aplicación la *Personal Information and Electronic Documents Act)*.
- Estados Unidos (solo cuando la entidad destinataria de los datos este certificada en el esquema del Escudo de Privacidad).

En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento **deben tomar medidas para compensar la falta de protección de datos** en un tercer país mediante garantías adecuadas para el interesado. Se deben poner a disposición de los interesados sus derechos exigibles y de acciones legales efectivas, incluyendo el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto.

¿Cómo cambia la situación con la llegada del RGPD?

Antes del RGPD, se obligaba a los exportadores de datos a solicitar una autorización previa para poder transferir datos a importadores establecidos en países que NO contaban con un nivel adecuado de protección, siempre que aporten las garantías suficientes, y a notificar las transferencias cuando se dirigen a países que sí disponen de dicho nivel adecuado.

Ahora con el RGPD, con carácter general, las transferencias se pueden llevar a cabo **sin necesidad de autorización previa**, salvo que las garantías se aporten a través de un **contrato** entre el responsable o el encargado del tratamiento, encargado o destinatario de los datos personales en el tercer país u organización internacional, o de un acuerdo administrativo entre autoridades públicas.

En el Reglamento se relacionan las garantías adecuadas que podrán ser aportadas sin que se requiera **ninguna autorización expresa** de una autoridad de control:

- Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
- Normas corporativas vinculantes.
- cláusulas tipo de protección de datos adoptadas por la Comisión;

- cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión;
- un código de conducta;
- un mecanismo de certificación.

Ahora bien, el RGPD establece una serie de excepciones que se deberán tener en cuenta.

Cloud computing y apps

Desde el punto de vista de protección de datos, **los prestadores de servicios de *cloud* tienen la consideración de encargados del tratamiento**, dado que, como consecuencia de la prestación de servicios de alojamiento, acceden a datos de carácter personal que son titularidad de sus clientes. Como consecuencia de lo anterior, es fundamental que en el **contrato de encargo de tratamiento** que se suscriba con el prestado de *cloud* se incluyan todas las menciones exigidas por la normativa.

Por otra parte, si el prestador de servicios se encuentra ubicado fuera de la Unión Europea, su acceso a los datos personales (por ejemplo, de clientes de una empresa que ha contrato sus servicios de alojamiento) conlleva una **transferencia internacional** de datos que requerirá la autorización del director de la Agencia Española de Protección de Datos.

Habrá que cumplir lo establecido en el RGPD respecto al encargo de tratamiento. Los encargados de tratamiento de proveedores tecnológicos de *cloud* (no comunitarios) desde hace un par de años han estado trabajando en **la implantación del RGPD adaptándose a las exigencias que el legislador europeo ha marcado**. Para muchos de ellos, ha supuesto una gran inversión económica, pero les ha supuesto una ventaja competitiva respecto al resto de proveedores tecnológicos. Cumplir con la normativa es garantía de éxito frente a clientes y terceros.

El proveedor *cloud* como encargado de tratamiento también deberá cumplir con la adopción de medidas técnicas (anonimización, cifrado, etc) y organizativas (DPO, formación, certificación, adhesión a códigos de conducta y un largo etc).

El cliente *cloud* (por ejemplo, un hospital) deberá ser cuidadoso a la hora de elegir su proveedor tecnológico y deberá «homologarle» y analizar si cumple con la normativa vigente y sus exigencias.

Por su parte, el uso de *apps* también tiene importantes implicaciones en materia de protección de datos. Las agencias de protección de datos europeas aprobaron en 2013 un dictamen señalando los retos que implica para la protección de la privacidad de los usuarios el uso de *apps* e impone una serie de obligaciones a todos los sujetos intervinientes en el desarrollo y uso de *apps* (desarrolladores, tiendas, fabricantes de *smarts* y creadores de sistemas operativos).

En este punto será de máxima importancia contemplar los **principios del RGPD y las medidas de responsabilidad proactiva contempladas como la privacidad desde el diseño y por el defecto, la realización del análisis de riesgo, realización de evaluación de impacto, etc...** (se explicarán en el próximo tema).

Lo + recomendado

No dejes de leer…

Publicidad no deseada

La Agencia Española de Protección de Datos nos da unas pautas de cómo dejar de recibir publicidad no deseada.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/areas/publicidad/index.html

Eliminar fotos y vídeos de Internet

La Agencia Española de Protección de Datos responde la siguiente cuestión: ¿Sabes cómo solicitar la eliminación de fotos o de vídeos publicados en internet? Tu imagen es un dato personal, tanto si apareces en una foto como en un vídeo.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/areas/internet/eliminar-fotos-y-videos-de-internet.html

Derecho de supresión (al olvido): buscadores de internet

La Agencia Española de Protección de Datos nos explica que el derecho a solicitar, bajo ciertas condiciones, que los enlaces a tus datos personales no figuren en los resultados de una búsqueda en internet realizada por tu nombre

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/areas/internet/derecho-al-olvido.html

Ejerce tus derechos

La Agencia Española de Protección de Datos nos explica que la normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión («derecho al olvido»), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/reglamento/derechos/index.html

Guías para el ciudadano

La Agencia Española de Protección de Datos nos presenta una guía para informar a los ciudadanos acerca de sus derechos en relación con el tratamiento de sus datos de carácter personal, así como el asesoramiento en la presentación de denuncias y reclamaciones, y cualquier otra cuestión que esté relacionada con el citado tratamiento.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-ciudadano.pdf

Guías videocámaras y seguridad

La Agencia Española de Protección de Datos nos presenta una guía sobre el uso de videocámaras para seguridad y otras finalidades

Accede al documento a través del aula virtual o desde la siguiente dirección web:
https://www.aepd.es/media/guias/guia-videovigilancia.pdf

No dejes de ver…

¿Por qué me vigilan, si no soy nadie?

Marta Peirano avisa en esta charla que es urgente preocuparse y proteger nuestro anonimato en la red.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=NPE7i8wuupk

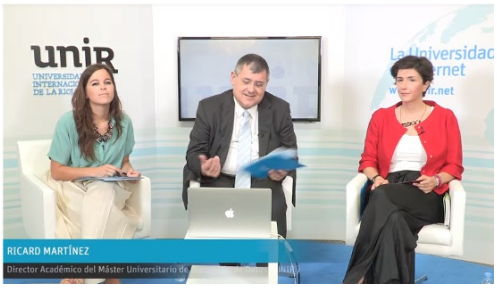
Cómo Cambridge Analytica analizó la personalidad de millones de usuarios de Facebook

Un modelo de psicología y un algoritmo de extraordinaria precisión sirvieron a Cambridge Analytica para analizar los perfiles de millones de usuarios de Facebook e intentar influenciar en sus votos. ¿Pero cómo analizó los datos de esos millones de usuarios? El modelo de los cinco grandes rasgos de personalidad, que se utiliza en psicología, le sirvió de base.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=7831NGClsrM

El impacto del Nuevo Reglamento Europeo de Protección de Datos en el sector digital

Openclass *El impacto del Nuevo Reglamento Europeo de Protección de Datos de la Unión Europea en el sector digital*. a cargo de Paula Ortíz, responsable de la dirección jurídica y de relaciones institucionales de IAB Spain y de Lucía Conde, Legal Counsel en Huawei Technologies. Moderada por Ricard Martínez, director del Máster Universitario de Protección de datos de UNIR.



Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=VLCTvGb04_0

El futuro del derecho de las TIC y la protección de datos

En esta *openclass* analizaremos cómo la evolución tecnológica y la necesidad de proteger los datos afecta al área jurídico-legal sobre todo tras el impacto de las TIC en las empresas. Hablaremos sobre *cloud computing*, inteligencia artificial (*machine learning y deep learning*), el *Internet of Things* (*wearables, asistentes inteligentes*) y la ciberseguridad.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=wZyqT25LxPk

+ Información

A fondo

El Reglamento General de Protección de Datos (RGPD)

En el siguiente enlace podemos encontrar el Reglamento General de Protección de Datos.

Accede al Reglamento a través del aula virtual o desde la siguiente dirección:
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Guía listado de cumplimiento normativo

Guía de la Agencia Española de Protección de Datos del listado de cumplimiento normativo.

Accede a la guía a través del aula virtual o desde la siguiente dirección:
https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf

STC 254/1993 (Libertad Informática)

Sentencia 254/1993, de 20 de julio. (BOE núm. 197).

Accede a la guía a través del aula virtual o desde la siguiente dirección:
http://hj.tribunalconstitucional.es/HJ/el-GR/Resolucion/Show/SENTENCIA/1993/254

STC 292/2000 (El derecho de protección de datos como derecho fundamental)

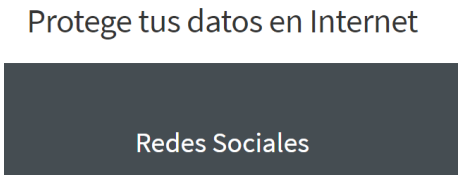
Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica.

Accede a la guía a través del aula virtual o desde la siguiente dirección:
https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

Enlaces relacionados

Como configurar la privacidad en las redes sociales

Página con diferentes vídeos para proteger tus datos en las redes sociales.



Accede a la página web a través del aula virtual o desde la siguiente dirección:
https://www.aepd.es/videos/index.html

Test

1. ¿Cuál de las siguientes conforme a la normativa de protección de datos no es fuente accesible al público?

A. El censo promocional.

B. Los boletines oficiales.

C. Internet.

D. La lista con los nombres de las personas que integran el Colegio de Abogados de Madrid.

2. La «libertad informática»:

A. Es el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data).

B. Comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

C. Está recogido en el art. 18.4 CE.

D. Todas las anteriores.

3. Según el nuevo Reglamento europeo, el consentimiento debe ser**:**

A. Libre, tácito, informado.

B. Libre, específico, informado e inequívoco.

C. Libre y específico valiendo las casillas preseleccionadas.

D. Ninguna de las anteriores.

4. Los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física son:

A. Datos genéticos.

B. Datos biométricos.

C. Datos disociados.

D. Datos sensibles.

5. Los datos personales obtenidos a partir de una muestra biológica son:

A. Datos genéticos.

B. Datos biométricos.

C. Datos disociados.

D. Datos sensibles.

6. El principio de minimización se refiere expresamente a:

A. La cantidad limitada de los datos recogidos.

B. El número de personas que acceden a los mismos.

C. El periodo del tratamiento.

D. Las tres anteriores.

7. Las políticas protección de datos personales asumidas por un responsable o encargado en la UE para 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 son:

A. Códigos de conducta.

B. *Best practices*.

C. Normas Vinculantes corporativas.

D. Código ético empresarial.

8. *Microsoft Azure* proveedor de *cloud computing* y encargado del tratamiento según el RGPD:

A. No recurrirá a otro encargado sin la autorización por escrito, específica o general, del responsable.

B. El tratamiento se regirá por un contrato con el responsable donde se establecerá el objeto, duración, finalidad del tratamiento, tipo de datos y categorías de interesados, obligaciones y derechos del responsable.

C. Si infringe dicho reglamento al determinar los fines y medios del tratamiento será considerado Responsable

D. Todas las anteriores son correctas.

9. Los prestadores de servicios de *cloud* tienen la consideración de:

A. Responsables del tratamiento.

B. Encargados del tratamiento.

C. Subencargados del tratamiento.

D. Titulares de datos personales.

10. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento:

A. Se deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado.

B. Se deben poner a disposición de los interesados sus derechos exigibles y de acciones legales efectivas, incluyendo el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país.

C. Se deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto.

D. Todas las anteriores.