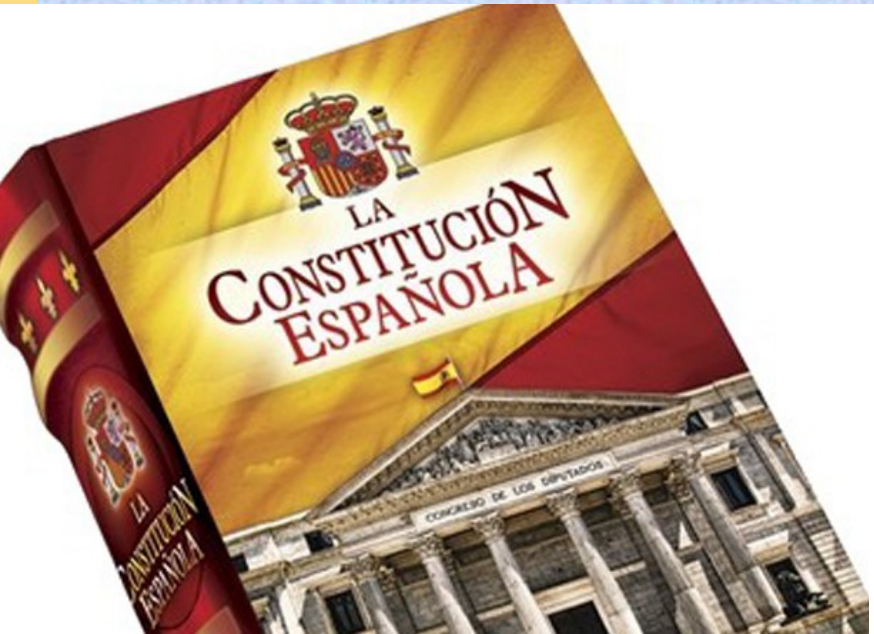
PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.

- La **PROTECCIÓN DE LAS PERSONAS FÍSICAS** en relación con el **TRATAMIENTO DE DATOS PERSONALES** es un **DERECHO FUNDAMENTAL** protegido por el **artículo 18.4 de la Constitución española.**



- TÍTULO I. De los derechos y deberes fundamentales
  - CAPÍTULO I. De los españoles y los extranjeros
  - CAPÍTULO II. Derechos y libertades
    - SECCIÓN 1. De los derechos fundamentales y de las libertades públicas
    - SECCIÓN 2. De los derechos y deberes de los ciudadanos
  - CAPÍTULO III. De los principios rectores de la política social y económica
  - CAPÍTULO IV. De las garantías de las libertades y derechos fundamentales
  - CAPÍTULO V. De la suspensión de los derechos y libertades

Privacidad

El Art. 18 de la "Constitución española de 1978" establece:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

PROTECCIÓN CONSTITUCIONAL DE DATOS PERSONALES

- Nuestra **CONSTITUCIÓN** reconoce el **DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES** cuando dispone que «**la ley** limitará el uso de **la informática** para garantizar **el HONOR y la INTIMIDAD PERSONAL Y FAMILIAR** de **los ciudadanos** y el pleno ejercicio de sus derechos».

Intimidad

Honor

Imagen

Ley Orgánica 1/1982, 5 de mayo, de PROTECCIÓN CIVIL DEL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y FAMILIAR Y A LA PROPIA IMAGEN.

DERECHO AL HONOR

- **Derecho fundamental** relacionado con la **INTIMIDAD PERSONAL Y FAMILIAR y LA PROPIA IMAGEN.**
- Pertenece a la **esfera privada de la persona** y constituye un bien integrante de los **DERECHOS DE LA PERSONALIDAD DEL INDIVIDUO.**

DERECHO A LA INTIMIDAD

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

Ley Orgánica 1/1982, 5 de mayo, de PROTECCIÓN CIVIL del DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y FAMILIAR Y A LA PROPIA IMAGEN.

- El **DERECHO A LA IMAGEN** es un **derecho personalísimo** que surge como una emanación de la personalidad.
- Es **lo que cada persona quiere mostrar de sí mismo ante los demás en cuánto a su aspecto**

III
II
70%
IV
V
35%
7k
50%

GDPR

25 MAY 2018
General
Data
Protection
Regulation

LEY PROTECCION DE DATOS 2018

NORMATIVA APLICABLE
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

- **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) o **RGPD.**

NORMATIVA APLICABLE PD

- Ley Orgánica 3/2018, de 5 de diciembre, de **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.**

Las 15 novedades que debes tener en cuenta sobre la

Nueva LOPDP

(Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de los Derechos Digitales):

vodafone business

ideasparatuempresa.es

"La **LOPD y el RGPD no son normativas excluyentes, sino complementarias** y de obligado cumplimiento para empresas y Administraciones"

SOCIEDAD DE LA INFORMACIÓN

- **Ley 34/2002, de 11 de julio, de SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO**

Ley 9/2014, de 9 de mayo, General de TELECOMUNICACIONES

LA LEY 9/2014, GENERAL DE TELECOMUNICACIONES.
TÍTULO I. DISPOSICIONES GENERALES.

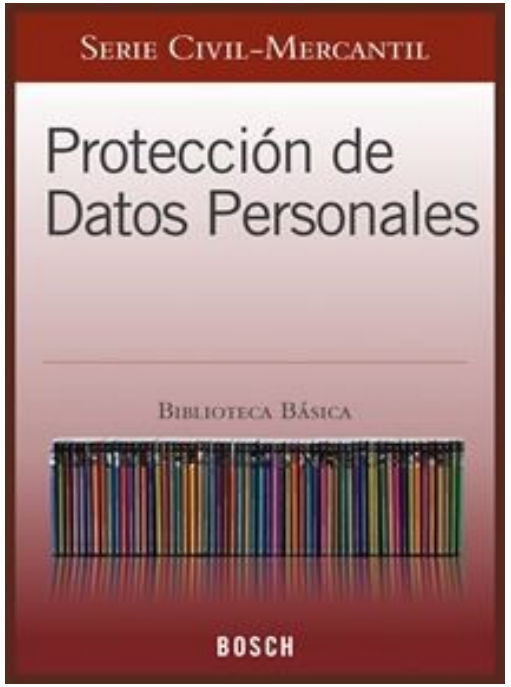
1 – Objetivos y principios (12)

- Fomentar la competencia efectiva en los mercados de telecomunicaciones
- Desarrollar la economía y el empleo digital, promover el desarrollo del sector de las telecomunicaciones y de todos los nuevos servicios digitales que las nuevas redes ultrarrápidas permiten.
- Promover el despliegue de redes y la prestación de servicios de comunicaciones electrónicas.
- Promover el desarrollo de la industria de productos y equipos de telecomunicaciones.
- Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la UE.
- Promover la inversión eficiente en infraestructuras.
- Posibilitar el uso eficaz de los recursos limitados de telecomunicaciones (numeración y espectro).
- Fomentar la neutralidad tecnológica.
- Garantizar el cumplimiento de las obligaciones de servicio público.
- Defender los intereses de los usuarios, asegurando derecho de acceso a servicios de comunicaciones electrónicas (elección, precio y buena calidad).
- Salvaguardar y proteger las necesidades de grupos sociales específicos.
- Facilitar el acceso de los usuarios con discapacidad a los servicios de comunicaciones electrónicas.

Protección de Datos:
Guía para el Ciudadano

ESPECIAL
Protección de datos
Guía para afrontar la nueva regulación
Wolters Kluwer

BOSCH
El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos
Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017
Coordinador
José López Calvo
Wolters Kluwer


Serie Civil-Mercantil
Protección de Datos Personales
Biblioteca Básica
BOSCH

TEXTOS LEGALES BÁSICOS
LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES
Y
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS
1ª EDICIÓN 2019
Contienen concordancias e índices analíticos
COLEX READER
Ebook + Actualizaciones en www.colex.es
COLEX

Las 30 claves de la protección de datos
Wolters Kluwer

CÓDIGO SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
4.ª edición, 2019
ARANZADI

DERECHO de PROTECCIÓN DE DATOS PERSONALES (T.C.)

- **Sentencia 94/1998, de 4 de mayo del TRIBUNAL CONSTITUCIONAL :**
- Existe un **DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS** por el que **se garantiza a la persona el control sobre sus datos**, cualesquiera datos personales, y sobre su uso y destino, **para evitar el tráfico ilícito de los mismos o lesivo para la dignidad** y los **derechos de los afectados**.

DERECHO de PROTECCIÓN DE DATOS PERSONALES (T.C.)

- **EL DERECHO A LA PROTECCIÓN DE DATOS** se configura como **una facultad del ciudadano para oponerse a que sus datos personales sean usados para fines distintos a aquel que justificó su obtención.**

El Derecho de la Protección de Datos implica garantía al sujeto de controlar sus datos personales, su uso y destino, para impedir el tráfico ilícito.

JURISPRUDENCIA DERECHO PD PERSONALES

- **SENTENCIA TC 292/2000, de 30 de noviembre:**
- Se considera como **un derecho autónomo e independiente** que consiste en **un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero**, sea el Estado o un particular, o cuáles puede este tercero recabar,
- también **permite al individuo** **saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.**

ANTECEDENTES REGULACION DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

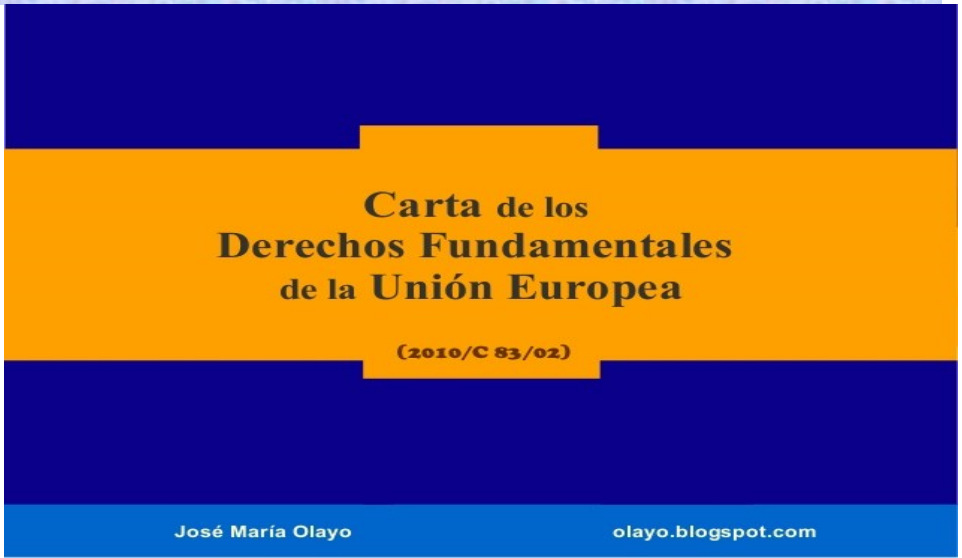
- A **nivel legislativo**, la concreción y desarrollo del **DERECHO FUNDAMENTAL DE PROTECCIÓN DE LAS PERSONAS FÍSICAS EN RELACIÓN CON EL TRATAMIENTO DE DATOS PERSONALES** tuvo lugar en sus orígenes mediante la aprobación de la **Ley Orgánica 5/1992, de 29 de octubre, reguladora del TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES**, conocida como **LORTAD.**

ANTECEDENTES REGULACION DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

- Fue reemplazada por la **Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales**, a fin de trasponer a nuestro derecho a la **Directiva 95/46/CE** del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Esta **ley orgánica** se complementó con una abundante **JURISPRUDENCIA procedente de los ÓRGANOS DE LA JURISDICCIÓN CONTENCIOSO-ADMINISTRATIVA.**

REGULACION EUROPEA DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

- Se recoge en el **artículo 8 de la CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA** y en el **artículo 16.1 del TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA (UE).**



CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

NIVEL DE PROTECCIÓN (art. II-113)

Dado que los derechos de la Carta también están en otros Tratados internacionales, en el Derecho Comunitario y en las Constituciones de los Estados miembros,

Se tiene que aplicar el nivel de protección más alto

que encontramos comparando los siguientes textos:

Convenio Europeo de Derechos Humanos

Derecho comunitario

Otros tratados internacionales

Constitución

REGULACION EUROPEA DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

- Anteriormente, **a nivel europeo**, se había adoptado la **Directiva 95/46/CE** citada, cuyo **objeto** era procurar que la **GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES** no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un **ESPACIO COMÚN DE GARANTÍA DEL DERECHO** que asegurase que en caso de **TRANSFERENCIA INTERNACIONAL DE LOS DATOS,** Su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia **directiva**.

REGULACION EUROPEA DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

- En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr **una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada.**
- El último hito en esta evolución tuvo lugar con la adopción 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 sus datos personales y a la libre circulación de estos datos** y por el que **se deroga** varias Directivas comunitarias.

Reglamento
General de
Protección
de Datos
GDPR

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

- El **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS** pretende **con su eficacia directa** superar los obstáculos que impidieron la finalidad armonizadora de la **Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995**, relativa a la **protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. (DEROGADA).**
- La **TRANSPOSICIÓN DE LA DIRECTIVA POR LOS ESTADOS MIEMBROS** se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la **Unión Europea** lo que ha conducido a que **existan diferencias apreciables en la protección de los derechos de los ciudadanos.**

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RPD)

- Se atiende a nuevas circunstancias, principalmente **el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior**, los retos planteados por **la rápida evolución tecnológica y la globalización**, que ha hecho que los **DATOS PERSONALES** sean el recurso fundamental de la sociedad de la información.
- El **carácter central de la información personal** tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos.
- Pero **tiene también RIESGOS**, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

- El **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS** supone **la revisión de las bases legales** del **MODELO EUROPEO DE PROTECCIÓN DE DATOS** más allá de una mera actualización de la vigente normativa.
- Procede a **REFORZAR LA SEGURIDAD JURÍDICA Y TRANSPARENCIA** a la vez que permite que sus normas sean especificadas o restringidas por el **Derecho de los Estados miembros** en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

- Así, el **REGLAMENTO (RGPD)** contiene un buen número de **habilitaciones**, cuando no imposiciones, **a los Estados miembros**, a fin de regular determinadas materias, permitiendo incluso, y a diferencia de lo que constituye **principio general del Derecho de la Unión Europea** que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el **Derecho de los Estados miembros**, estos tengan la posibilidad de incorporar **al Derecho nacional** previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

- No se excluye toda **intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos**.
- Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para **la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento** de que se trate.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

- El **PRINCIPIO DE SEGURIDAD JURÍDICA**, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de **eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo**.
- De esta segunda vertiente se colige la consiguiente **OBLIGACIÓN DE DEPURAR EL ORDENAMIENTO JURÍDICO.**

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

- En definitiva, el **PRINCIPIO DE SEGURIDAD JURÍDICA** obliga a que la normativa interna que resulte incompatible con el **DERECHO DE LA UNIÓN EUROPEA** quede definitivamente eliminada «*mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse*» (**Sentencias del Tribunal de Justicia**).
- Por último, **LOS REGLAMENTOS**, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras **normas internas complementarias** para hacer plenamente efectiva su aplicación.
- En este sentido, **más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.**

Ley Orgánica 3/2018, de 5 de diciembre, de **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES**

- La **ADAPTACIÓN** al **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS**, que era aplicable a partir del **25 de mayo de 2018**, según su artículo 99, requería **la elaboración de una NUEVA LEY ORGÁNICA que sustituya a la actual.**
- En esta labor se han preservado **LOS PRINCIPIOS DE BUENA REGULACIÓN**, al tratarse de una norma necesaria para **la adaptación del ordenamiento español a la citada disposición europea** y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

DECLARACIÓN DE LOS DERECHOS DEL HOMBRE Y DEL CIUDADANO EN INTERNET

DECLARACIÓN DE LOS DERECHOS DEL HOMBRE Y DEL CIUDADANO EN INTERNET

- **INTERNET** se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva.
- Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en **la Red** y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad.
- Ya en los años 90, y conscientes del **impacto que iba a producir Internet en nuestras vidas**, los pioneros de la Red propusieron elaborar una **DECLARACIÓN DE LOS DERECHOS DEL HOMBRE Y DEL CIUDADANO EN INTERNET.**

MAYO Día de 17

INTERNET

www.diadeinternet.org

DÍA MUNDIAL DE LAS TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN

FÉNIX DIRECTO

Una compañía de Allianz

hp

Telefónica

Google

El Corte Inglés

facebook

DERECHOS DE LA CIUDADANÍA EN INTERNET

- Hoy identificamos con bastante claridad los **riesgos y oportunidades** que **EL MUNDO DE LAS REDES** ofrece a la ciudadanía.
- Corresponde a **los poderes públicos** impulsar políticas que hagan efectivos **LOS DERECHOS DE LA CIUDADANÍA EN INTERNET** promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital.
- La **TRANSFORMACIÓN DIGITAL DE NUESTRA SOCIEDAD** es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico.
- En este contexto, países de nuestro entorno ya han aprobado **normativa** que refuerza **los DERECHOS DIGITALES DE LA CIUDADANÍA.**

LOS DERECHOS DIGITALES SON DERECHOS HUMANOS

RESOLUCIÓN 68/167 DEL CONSEJO DE DERECHOS HUMANOS DE LA ASAMBLEA GENERAL DE LAS NACIONES UNICAS, | JULIO DE 2016

RECONOCIMIENTO DE UN SISTEMA DE GARANTÍA DE LOS DERECHOS DIGITALES

- Los **CONSTITUYENTES DE 1978** ya intuyeron el enorme impacto que **los avances tecnológicos** provocarían en nuestra sociedad y en el disfrute de los derechos fundamentales.
- Una deseable **FUTURA REFORMA DE LA CONSTITUCIÓN** debería incluir entre sus prioridades **LA ACTUALIZACIÓN DE LA CONSTITUCIÓN A LA ERA DIGITAL** y, específicamente, elevar a rango constitucional **una nueva generación de derechos digitales.**

RECONOCIMIENTO DE UN SISTEMA DE GARANTÍA DE LOS DERECHOS DIGITALES

- Pero, en tanto no se acometa este reto, **el legislador** aborda **el RECONOCIMIENTO DE UN SISTEMA DE GARANTÍA DE LOS DERECHOS DIGITALES** que encuentra su anclaje en el mandato impuesto por el **apartado 4º del artículo 18 de la Constitución Española** y que, en algunos casos, ya han sido perfilados por **la JURISPRUDENCIA ORDINARIA, CONSTITUCIONAL Y EUROPEA.**

BOLETÍN OFICIAL DEL ESTADO
Núm. 294 Jueves 6 de diciembre de 2018 Sec. I. Pág. 119788

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

16673 *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

Ley Orgánica 3/2018, de 5 de diciembre, de **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES**

OBJETO DE LA LEY ORGÁNICA.

- **1º** se pretende **lograr LA ADAPTACIÓN del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS, y completar sus disposiciones.**
- A su vez, establece que **el DERECHO FUNDAMENTAL DE LAS PERSONAS FÍSICAS A LA PROTECCIÓN DE DATOS PERSONALES**, amparado por el **artículo 18.4 de la Constitución**, se ejerce con arreglo a lo establecido en el **Reglamento (UE) 2016/679 y en la ley orgánica.**

OBJETO DE LA LEY ORGÁNICA.

- Las **COMUNIDADES AUTÓNOMAS** ostentan **competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad,** y a las **AUTORIDADES AUTONÓMICAS DE PROTECCIÓN DE DATOS** que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía.
- **2°** objeto de la ley **GARANTIZAR LOS DERECHOS DIGITALES DE LA CIUDADANÍA,** al amparo de lo dispuesto en el **artículo 18.4 de la Constitución.**

Las 15 novedades que debes tener en cuenta sobre la

Nueva LOPDP

(Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de los Derechos Digitales):

Ley Orgánica 3/2018, de 5 de diciembre, de **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES**

Novedosa regulación de los **DATOS REFERIDOS A LAS PERSONAS FALLECIDAS:**

- **EXCLUYE DEL ÁMBITO DE APLICACIÓN DE LA LEY SU TRATAMIENTO,**

¿Qué hacer cuando alguien se muere?

Guía definitiva

RESUMEN DE TRÁMITES NECESARIOS ANTES DEL ENTIERRO O INCINERACIÓN DEL CUERPO DE LA PERSONA FALLECIDA

- **Certificado Médico de Defunción (CMD)** – Si la persona fallece en la **Unidad de Cuidados Intensivos de un hospital,** se le pregunta a la familia si firma o no el Consentimiento Familiar para la donación de órganos, si ésta considera que era la voluntad del fallecido o no. En caso de que el fallecido sea apto para la donación de órganos.
- **Inscripción del fallecido en el Registro Civil** con el CMD.
- Solicitud y Obtención de **la Licencia de Enterramiento**.
- **Traslado del cadáver hasta el cementerio o crematorio**.
- **Enterramiento o incineración del cuerpo**, con o sin Funeral Religioso previo, dependiendo de las creencias del fallecido y/o la familia.

RESUMEN DE TRÁMITES NECESARIOS DESPUÉS DEL ENTIERRO O INCINERACIÓN DE LA PERSONA FALLECIDA

- **Certificado de Actos de Última Voluntad**
- **Certificado de Contratos de Seguro de Cobertura de Fallecimiento.**
- **Testamento o Declaración de Herederos.**
- **Inventario**(descripción de los bienes de la herencia y valoración éstos)
- Realización del **cuaderno particional y designación de cada haber hereditario.**
- **Pago de impuestos.**
- **Impuesto de sucesiones**
- **Impuesto sobre el incremento de valor de terrenos de naturaleza urbana** (antigua plusvalía municipal)
- **Toma de posesión de los bienes de la herencia.**
- **Solicitud de prestaciones y pensiones.**

DATOS REFERIDOS A LAS PERSONAS FALLECIDAS

- Pero **se permite** que **las PERSONAS VINCULADAS AL FALLECIDO por razones familiares o de hecho, o sus herederos** puedan **solicitar el acceso a los mismos**, así como **su rectificación o supresión**, en su caso **con sujeción a las INSTRUCCIONES DEL FALLECIDO**.

Ley Orgánica 3/2018, de 5 de diciembre, de **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES**

- También **EXCLUYE del ámbito de aplicación** los **TRATAMIENTOS QUE SE RIJAN POR DISPOSICIONES ESPECÍFICAS**, en referencia a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria 4ª la aplicación a estos tratamientos de la **Ley Orgánica 15/1999, de 13 de diciembre**, hasta que se apruebe la citada normativa.

LOS NUEVOS DERECHOS DIGITALES RECONOCIDOS POR LA LEY ORGÁNICA 3/2018

- La **nueva Ley Orgánica 3/2018, de 5 de diciembre, de PROTECCIÓN DE DATOS Y GARANTÍA DE LOS DERECHOS DIGITALES**, además de destinarse a **ADAPTAR** EL ORDENAMIENTO ESPAÑOL al **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS** y completar sus disposiciones, incorpora a su objeto la importante novedad de dirigirse a "**GARANTIZAR LOS DERECHOS DIGITALES DE LA CIUDADANÍA** establecido en el **artículo 18.4 de la Constitución**"

NUEVA LEY DE PROTECCIÓN DE DATOS

El pasado 6 de diciembre por fin fue publicada en el BOE.
¿Conoces los nuevos derechos digitales que garantizan
la seguridad de tus datos en Internet?

GARANTÍA DE LOS DERECHOS DIGITALES

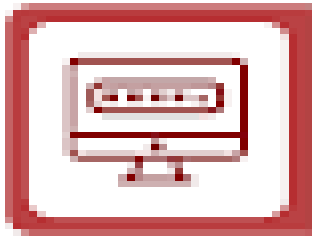
Se reconoce y regula el **ejercicio de derechos** como:

- El de **NEUTRALIDAD DE LA RED,** y el **ACCESO UNIVERSAL a INTERNET,**
- **LOS DERECHOS A LA SEGURIDAD Y EDUCACIÓN DIGITAL,**
- **LA LIBERTAD DE EXPRESIÓN EN INTERNET,**
- **EL DERECHO AL OLVIDO EN BUSCADORES Y REDES SOCIALES,**
- **DERECHO A LA PORTABILIDAD,**
- **DERECHO AL TESTAMENTO DIGITAL,**
- **DERECHO A LA INTIMIDAD EN EL USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL Y A LA DESCONEXIÓN DIGITAL.**

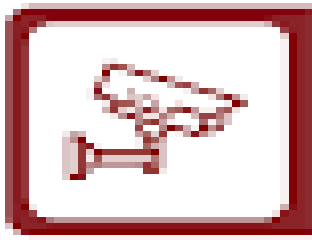
LOPD-GDD

DERECHOS DIGITALES DE LOS TRABAJADORES

DESCONEXIÓN DIGITAL FUERA DEL HORARIO DE TRABAJO



ACCESO POR LA EMPRESA A CONTENIDOS DEL TRABAJADOR



GRABACIÓN DEL EMPLEADO Y GEOLOCALIZACIÓN

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

COMPETENCIAS DE LA AEPD EN RELACIÓN CON LOS DERECHOS RECONOCIDOS EN EL TÍTULO X

- La **Ley Orgánica 3/2018** regula **LAS FUNCIONES Y POTESTADES DE LA AEPD.**
- Corresponde a la **autoridad administrativa independiente** **"supervisar la aplicación de la ley orgánica y del Reglamento (UE) 2016/679"** ejerciendo las funciones que tiene establecidas en el mismo y en la ley orgánica, y **quedan fuera de su ámbito de aplicación** los denominados **"DERECHOS EN LA ERA DIGITAL".**

COMPETENCIAS DE LA AEPD EN RELACIÓN CON LOS DERECHOS RECONOCIDOS EN EL TÍTULO X

- **LA AGENCIA NO ES COMPETENTE EN RELACIÓN CON LOS DENOMINADOS "DERECHOS EN LA ERA DIGITAL"**, así como los **DERECHOS A LA NEUTRALIDAD DE INTERNET**; de **ACCESO UNIVERSAL A INTERNET**; a **LA SEGURIDAD DIGITAL**; a **la EDUCACIÓN DIGITAL**; a la **PROTECCIÓN DE LOS MENORES EN INTERNET**; el **DERECHO DE RECTIFICACIÓN EN INTERNET**; el **DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES**; el **DERECHO A LA INTIMIDAD Y USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL**; el **DERECHO A LA DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL** y **LOS DERECHOS DE PORTABILIDAD EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES**, el **DERECHO AL TESTAMENTO DIGITAL** y las **POLÍTICAS DE IMPULSO DE LOS DERECHOS DIGITALES.**

Garantía de los derechos digitales en la nueva LOPD
DCD.ES

GARANTÍA DE DERECHOS DIGITALES
DERECHO A LA NEUTRALIDAD DE INTERNET
DERECHO DE ACCESO UNIVERSAL A INTERNET
DERECHO A LA SEGURIDAD DIGITAL
PROTECCIÓN DE LOS MENORES EN INTERNET
DERECHO DE RECTIFICACIÓN EN INTERNET
DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES
DERECHOS DIGITALES EN EL ÁMBITO LABORAL
DERECHO A LA INTIMIDAD Y USO DE DISPOSITIVOS DIGITALES
DERECHO A LA DESCONEXIÓN DIGITAL
DERECHO A LA INTIMIDAD FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO
DERECHO A LA INTIMIDAD ANTE LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL
DERECHOS DIGITALES EN LA NEGOCIACIÓN COLECTIVA

COMPETENCIAS DE LA AEPD EN RELACIÓN CON LOS DERECHOS RECONOCIDOS EN EL TÍTULO X

- **LA GARANTÍA DE ESTOS DERECHOS Y LAS FACULTADES ATRIBUIDAS A SUS TITULARES** en virtud de esta norma deben recaer bajo la competencia de algún **ORGANISMO PÚBLICO determinado** por el correspondiente **desarrollo normativo.**

OBJETO DE LA LEY ORGÁNICA 3/2018

- **Adaptar** el ordenamiento jurídico español al **Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016**, relativo a la **protección de las personas físicas en lo que respecta al tratamiento de sus datos personales** y a **la libre circulación de estos datos**, y completar sus disposiciones.
- El **DERECHO FUNDAMENTAL DE LAS PERSONAS FÍSICAS A LA PROTECCIÓN DE DATOS PERSONALES**, amparado por el **artículo 18.4 de la Constitución**, se ejercerá con arreglo a lo establecido en **el Reglamento (UE) 2016/679** y en esta ley orgánica.
- **Garantizar los DERECHOS DIGITALES de la ciudadanía** conforme al mandato establecido en el **artículo 18.4 de la Constitución.**

DATOS EXCLUIDOS LOPD Y RGPD

Datos de las personas fallecidas (II)

Art. 18.4 de la Ley 41/2002, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica:

Sólo se facilitará el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite.

En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes.

No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

Buscar personas fallecidas
Rutificador.cl

DATOS DE LAS PERSONAS FALLECIDAS

DATOS DE LAS PERSONAS FALLECIDAS

- **REGLA GENERAL:**
- Las **PERSONAS VINCULADAS AL FALLECIDO POR RAZONES FAMILIARES O DE HECHO** así como **SUS HEREDEROS** pueden dirigirse **al responsable o encargado del tratamiento** al objeto de **solicitar el acceso a los datos personales de aquella** y, en su caso, **su rectificación o supresión.**

DATOS DE LAS PERSONAS FALLECIDAS

- **EXCEPCIÓN A LA REGLA GENERAL**:
- Las personas anteriores **no pueden acceder a los datos del causante,** ni solicitar su rectificación o supresión, **cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.**
- Dicha **PROHIBICIÓN** no afecta al **DERECHO DE LOS HEREDEROS a acceder** a los **DATOS DE CARÁCTER PATRIMONIAL DEL CAUSANTE.**

DATOS DE LAS PERSONAS FALLECIDAS

- **Las PERSONAS O INSTITUCIONES A LAS QUE EL FALLECIDO HUBIESE DESIGNADO EXPRESAMENTE PARA ELLO** pueden también **SOLICITAR,** con arreglo a **las instrucciones recibidas**, el acceso a los datos personales de este y, en su caso su rectificación o supresión.
- Mediante **REAL DECRETO** se establecerán los requisitos y condiciones para acreditar la validez y vigencia **de estos mandatos e instrucciones** y, en su caso, **el registro de los mismos**.

DATOS DE LAS PERSONAS FALLECIDAS

- En caso de **FALLECIMIENTO DE MENORES**, estas facultades pueden ejercerse también por sus **REPRESENTANTES LEGALES** o, en el marco de sus competencias, **por el MINISTERIO FISCAL**, que puede actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

DATOS DE LAS PERSONAS FALLECIDAS

- En caso de **FALLECIMIENTO DE PERSONAS CON DISCAPACIDAD**, estas **facultades** también pueden ejercerse, además de por **los anteriores**, por quienes hubiesen sido **DESIGNADOS PARA EL EJERCICIO DE FUNCIONES DE APOYO (CUIDADORES)**, si **tales facultades** se entendieran comprendidas en **las medidas de apoyo prestadas por el designado.**

¿Qué hacer con la información digital cuando alguien fallece?

Asesoría e

Glosario de términos RGPD

@lexblogger_

¿Qué son los datos personales?

- Identificación online
- Nombre y apellidos
- Datos bancarios
- Información sobre salud
- Dirección
- Localización
- •••

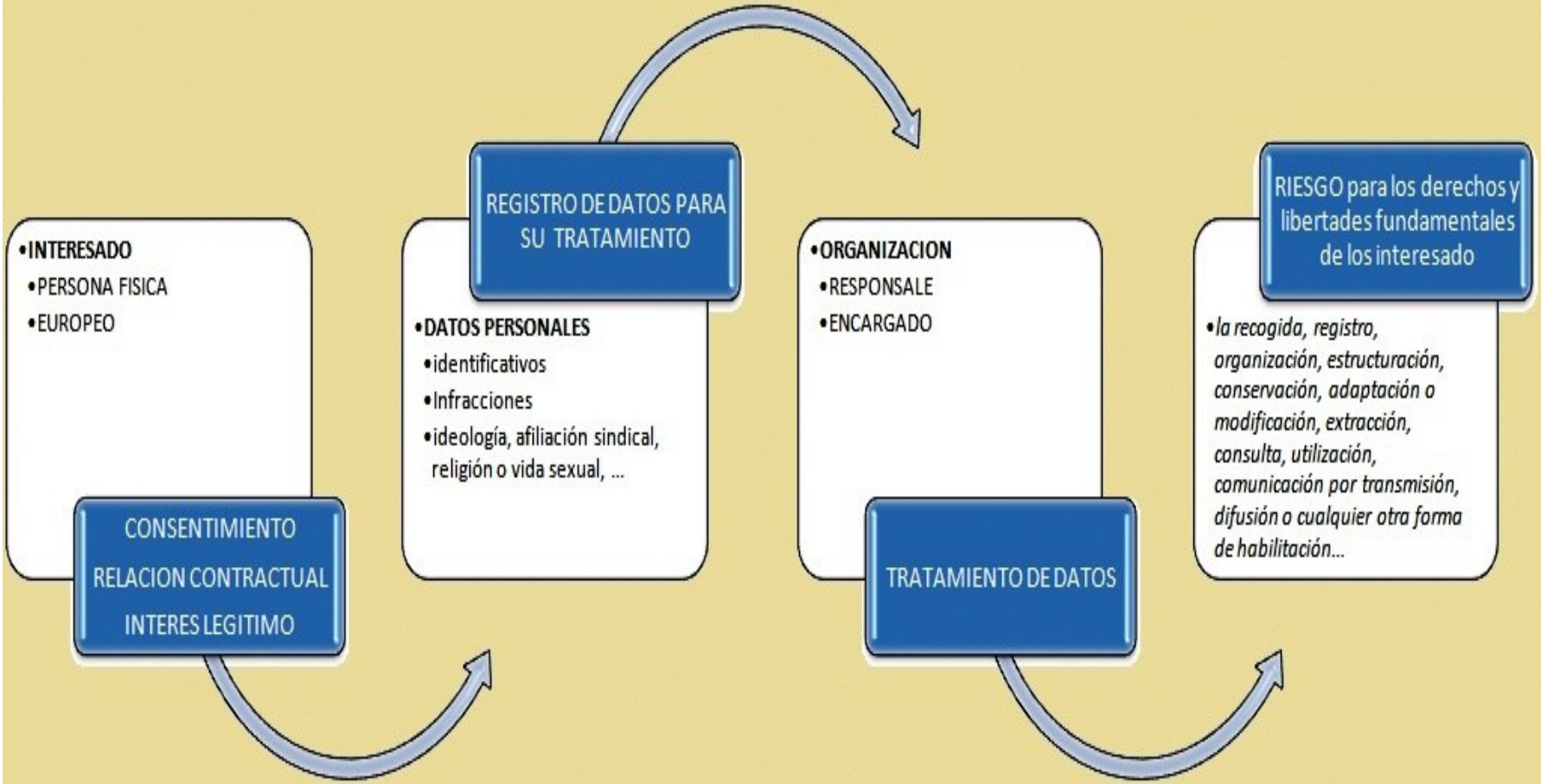
DATOS PERSONALES

- Toda información sobre una persona física identificada o identificable («**EL INTERESADO**»);
- Es **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;

TRATAMIENTO

- Cualquier **operación o conjunto de operaciones realizadas** sobre **DATOS PERSONALES O CONJUNTOS DE DATOS PERSONALES**, ya sea por procedimientos automatizados o no, tales 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 Personales



LIMITACIÓN DEL TRATAMIENTO

- El **MARCADO DE LOS DATOS DE CARÁCTER PERSONAL CONSERVADOS** con el fin de **limitar su tratamiento** en el futuro.

Derecho a la limitación del tratamiento

- **Consecuencias (art. 18.2):**
  - **Tratamiento limitado a la conservación salvo:**
    - **Consentimiento**
    - **Formulación, ejercicio o defensa de reclamaciones**
    - **Protección derechos de personas físicas o jurídicas**
    - **Interés público importante UE o EEMM**
  - **Comunicación a los destinatarios salvo imposibilidad o esfuerzo desproporcionado (art. 19)**
- **Derechos de los interesados**
  - **Ser informado antes del levantamiento de la limitación (art. 18.3)**
  - **Información sobre los destinatarios si el interesado lo solicita (art. 19)**

Agencia Española de Protección de Datos 17

ELABORACIÓN DE PERFILES

- Toda forma de **tratamiento automatizado** de **datos personales** consistente en **UTILIZAR DATOS PERSONALES PARA EVALUAR DETERMINADOS ASPECTOS PERSONALES DE UNA PERSONA FÍSICA**, en particular para **analizar o predecir aspectos** relativos al **rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física**;

PERFILADO O PROFILING

EL MANEJO DE LA INFORMACIÓN PERSONAL POR PARTE DE LAS EMPRESAS Y POR TANTO LA CREACIÓN DE PERFILES ES REALMENTE APASIONANTE Y PREOCUPANTE.

PERFIL del DPO*

1. **Conocimientos especializados en Derecho**
2. **Práctica en la protección de datos**
3. **Independiente**
4. **Con visión global**
5. **Que conozca el modelo de negocio de la empresa**
6. **Empático y orientado al cliente**
   Va a ser el punto de contacto, el enlace entre este cliente/ciudadano/usuario y la Agencia de control (AEPD) y entre éste y la empresa.
7. **En constante formación**
   Cuanto mayor sea la calidad de los conocimientos de estos profesionales mayor credibilidad tendrán y mayor valor se dará a su tarea. Debe tener claro su plan de formación constante y su plan de estrategia profesional (Universidad, asociaciones de profesionales, CGAE,...).
8. **Con capacidad para trabajar en equipo**
   Apuntaban a una persona con un perfil jurídico, dentro de un equipo multidisciplinar que apoya al jefe del equipo que tiene un perfil tecnológico.
9. **Que conozca la tecnología**
   Para evaluar los riesgos y establecer los controles de cumplimiento. Ya no sólo será el encargado de registrar ficheros de datos y hacer políticas de privacidad, debe encontrar las medidas técnicas y organizativas apropiadas.
10. **Proactivo**
11. **Con carácter anticipador**
12. **Legal**
    "verídico, puntual, fiel y recto en el cumplimiento de las funciones de su cargo" (según la RAE)
13. **Transversal**
    Se habla del abogado 360º
14. **Con capacidad para evolucionar e innovar**
15. **Con capacidad para elaborar mensajes claros a sus destinatarios**
    Cliente interno y cliente externo
16. **Buena capacidad de comunicación**
    Pensemos, por ejemplo, que ante una brecha de seguridad deberá comunicarse con los medios de prensa.

* Delegado de Protección de Datos.

Profesional de la privacidad

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

Infografía realizada por Sonsoles Valero para Juristas con Futuro

Reconocimientos y premios
Extracto
Diplomas
Publications
Proyectos
Experiencia
Educación
Organizaciones
Aptitudes y recomendaciones

Nuevos conceptos

- Resiliencia
  - "capacidad de soportar y recuperarse ante desastres"
- Seudonimización:
  - el tratamiento de datos personales de manera tal que:
    - ya no puedan 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;

SEUDONIMIZACIÓN

- El **TRATAMIENTO DE DATOS PERSONALES** de manera tal que ya **no puedan 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.**

Medidas previstas en el #RGPD:

- a) la seudonimización y el cifrado de datos personales;
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Niveles de seguridad

FICHERO

- Todo **CONJUNTO ESTRUCTURADO DE DATOS PERSONALES**, **accesibles** con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

Archivos o ficheros

Carpetas o directorios

RESPONSABLE DEL TRATAMIENTO

- Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento.**
- Si el **DERECHO DE LA UNIÓN O DE LOS ESTADOS MIEMBROS** determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento puede establecerlos el **Derecho de la Unión o de los Estados miembros.**

Procedimiento Administrativo
Las nuevas funciones del
responsable del fichero de datos

ENCARGADO DEL TRATAMIENTO

- la persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales por cuenta del responsable del tratamiento**;
- **Trabajar con terceros** es habitual en muchas empresas. Es necesario contratar a terceros para que realicen servicios que nuestra propia entidad no puede realizar y que se necesita para el día a día.
- Un **ejemplo** de esto podría ser cuando necesitamos contratar **un servicio informático para la instalación de nuestros sistemas**, o a una **gestoría para el pago de las nóminas a mis trabajadores.**

Responsables y Encargados

Responsable del fichero o tratamiento:

Empresa que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del Tratamiento:

Empresa que, sólo o conjuntamente con otros, trate datos personales **por cuenta del responsable del tratamiento**.

Encarga las nominas de los empleados

El empresario o Empresa
(Responsable del Fichero)

El Gestor
(Encargado del Fichero)

megasyc
software y comunicaciones

Responsable del tratamiento
Encargados
Subcontratados
Corresponsables
Destinatarios

¿QUÉ ES UN ACCESO A DATOS POR CUENTA DE TERCEROS?

- Se produce un **ACCESO A DATOS POR CUENTA DE TERCEROS** cuando la empresa recurre a una **entidad externa,** para que realice la **prestación de un servicio en su nombre.**
- **Este ACCESO** puede **implicar** el acceso a sus ficheros, o a los sistemas que contengan datos de carácter personal de su responsabilidad.
- **EJEMPLOS DE ENCARGADOS DEL TRATAMIENTO**:
  - contratación de servicios informáticos
  - prestación de servicios de buckups online
  - gestoría laboral y fiscal
  - servicios de marketing
  - prevención de riesgos laborales

Acceso a datos

- **¿Qué es el acceso a los datos por cuenta de terceros?** **(Art 12 de la LOPD y Art. 20, 21 y 22 del RD 1720/2007)**

-El responsable del fichero permite a un tercero acceder a los datos de carácter personal para que preste un servicio relacionado con los mismos.

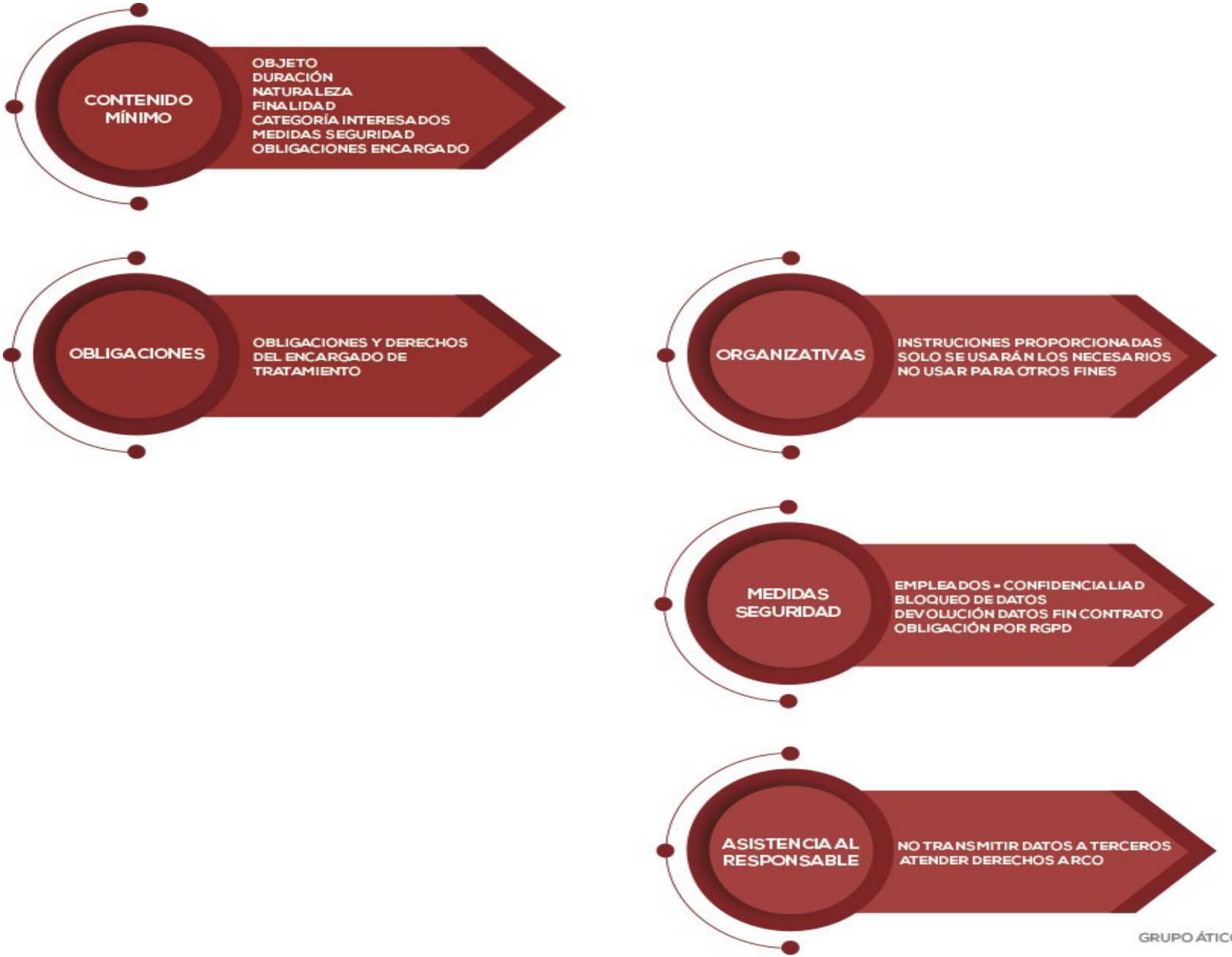
-El tercero, denominado encargado de tratamiento se limita a tratar los datos por cuenta del responsable de los datos, es decir siguiendo sus instrucciones y devolviendo o destruyendo los datos una vez finalizado el servicio contratado.

Ej: encargados de tratamiento serian las asesorías o gestorías que realizan la gestión contable, fiscal o laboral; servicios de Prevención de Riesgos; empresas de mantenimiento de Software o Hardware…

CONTRATOS DE ENCARGO DE TRATAMIENTO DE DATOS

ACCESO A DATOS POR CUENTA DE TERCEROS

GRUPO ÁTICO34


CONTENIDO MÍNIMO
OBJETO
DURACIÓN
NATURALEZA
FINALIDAD
CATEGORÍA INTERESADOS
MEDIDAS SEGURIDAD
OBLIGACIONES ENCARGADO
OBLIGACIONES
OBLIGACIONES Y DERECHOS DEL ENCARGADO DE TRATAMIENTO
ORGANIZATIVAS
INSTRUCIONES PROPORCIONADAS
SOLO SE USARÁN LOS NECESARIOS
NO USAR PARA OTROS FINES
MEDIDAS SEGURIDAD
EMPLEADOS - CONFIDENCIALIAD
BLOQUEO DE DATOS
DEVOLUCIÓN DATOS FIN CONTRATO
OBLIGACIÓN POR RGPD
ASISTENCIA AL RESPONSABLE
NO TRANSMITIR DATOS A TERCEROS
ATENDER DERECHOS ARCO

DESTINATARIO

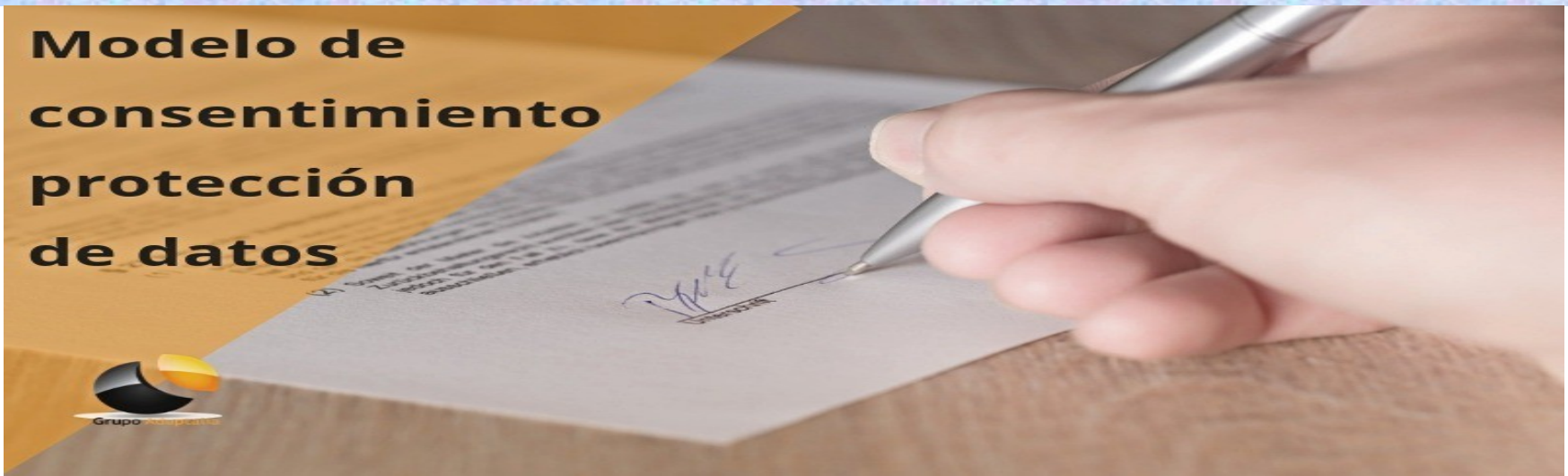
- Persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.
- No obstante, **NO SE CONSIDERAN DESTINATARIOS** las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros;
- El **tratamiento de tales datos por dichas autoridades públicas** será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

TERCERO

- Persona física o jurídica, autoridad pública, servicio u organismo **distinto del INTERESADO, del RESPONSABLE DEL TRATAMIENTO, del ENCARGADO DEL TRATAMIENTO** y de las **personas autorizadas para tratar los datos personales** bajo la autoridad directa del responsable o del encargado;

CONSENTIMIENTO DEL INTERESADO

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



Tipos de consentimiento

- Partimos de la base de que al interesado le informamos de lo que queremos hacer con sus datos. Después el interesado nos debe dar su consentimiento que puede ser:

- Consentimiento tácito
  - Si el interesado, una vez transcurrido un tiempo prudencial, más o menos 1 mes, desde que se le ha informado, no se manifiesta contrario al tratamiento, quiere decir que está dando el consentimiento tácito

- Consentimiento expreso (por escrito o no)
  - El interesado debe declarar "de forma clara e inequívoca que acepta o consiente el tratamiento o la cesión de los que se le informa, mediante la expresión de su voluntad. Podrá hacerlo **por escrito**, verbalmente, mediante comunicación telemática o por cualquier otro medio".

NO
SI
SI
SI
NO
NO
SI
NO
SI
NO
SI
SI

VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

- Toda **VIOLACIÓN DE LA SEGURIDAD** que ocasione **la destrucción, pérdida o alteración accidental o ilícita de datos personales** transmitidos, conservados o tratados de otra forma, o **la COMUNICACIÓN O ACCESO NO AUTORIZADOS a dichos datos**.

Incidentes de seguridad

Protocolo de actuación

6. DECISIÓN FINAL

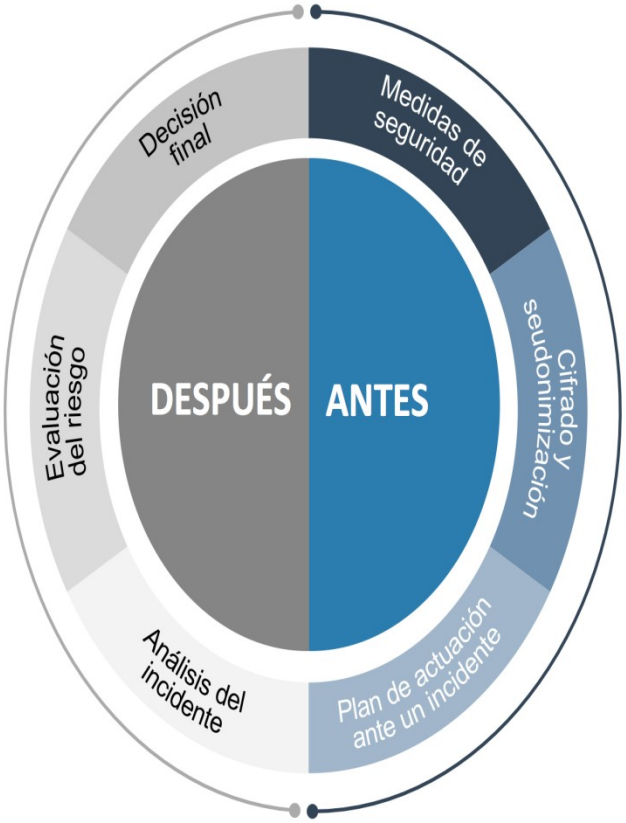
- □ Riesgo bajo: no notificar
- □ Riesgo alto: notificar a la AEPD
- □ Riesgo muy alto: comunicar a los afectados

5. EVALUACIÓN DEL RIESGO

- □ Tipo de violación de la seguridad
- □ Sensibilidad de los datos
- □ Gravedad del impacto para los afectados
- □ Facilidad de identificación

4. ANÁLISIS DEL INCIDENTE

- □ Alcance
- □ Número de afectados
- □ Origen
- □ Intencionalidad



1. MEDIDAS DE SEGURIDAD

- □ Política de seguridad
- □ Normas de seguridad
- □ Medidas organizativas
- □ Medidas ISO 27001

2. CIFRADO DE DATOS Y SEUDONIMIZACIÓN

- □ Datos ininteligibles
- □ Clave bien custodiada
- □ Datos disociados
- □ Intencionalidad

3. PLAN DE ACTUACIÓN ANTE UN INCIDENTE

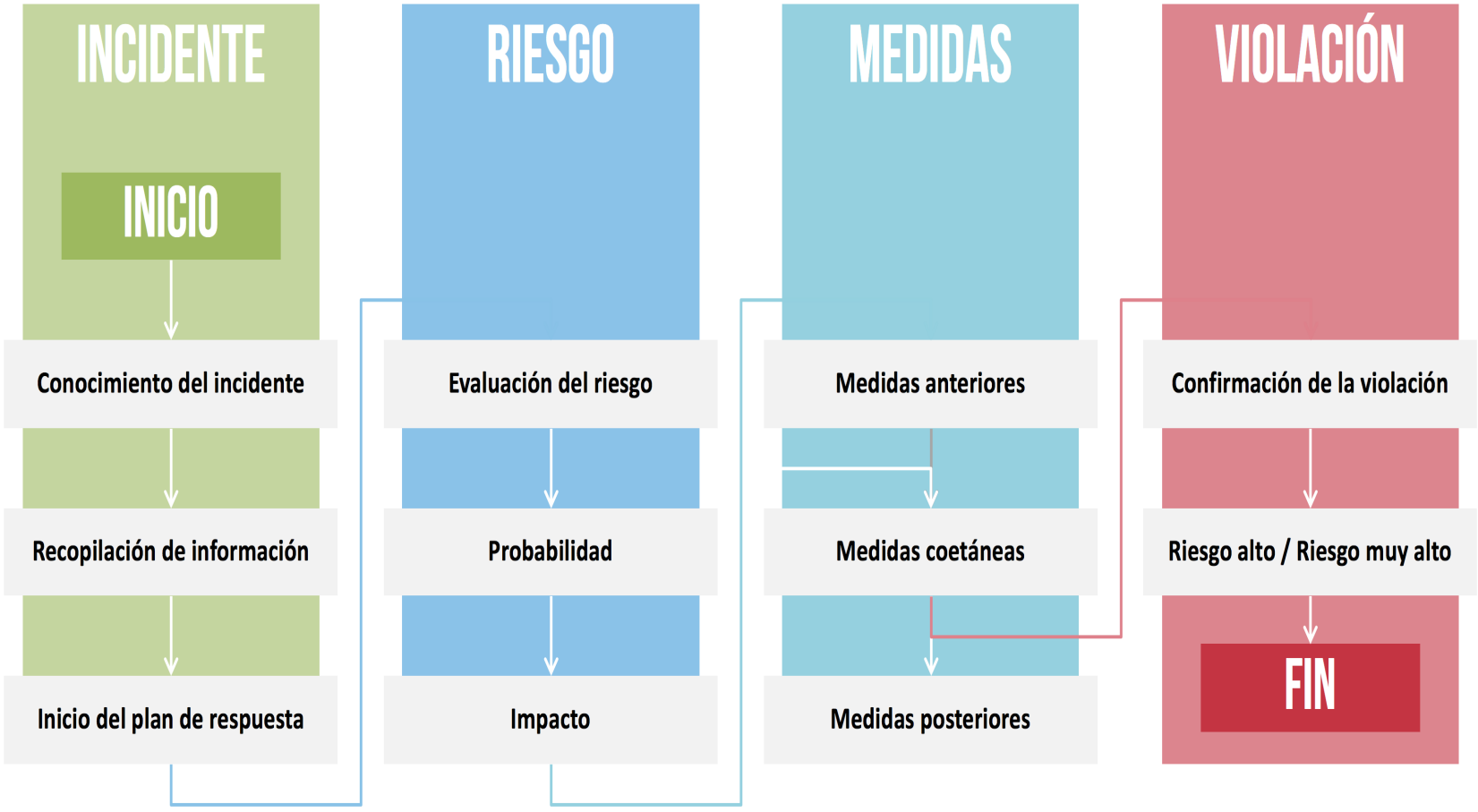
- □ Protocolo de actuación
- □ Responsables
- □ Tiempo de respuesta

© Copyright Xavier Ribas 2017

ribas 30 años 1987 - 2017

Evaluación de la violación de datos

Protocolo de actuación



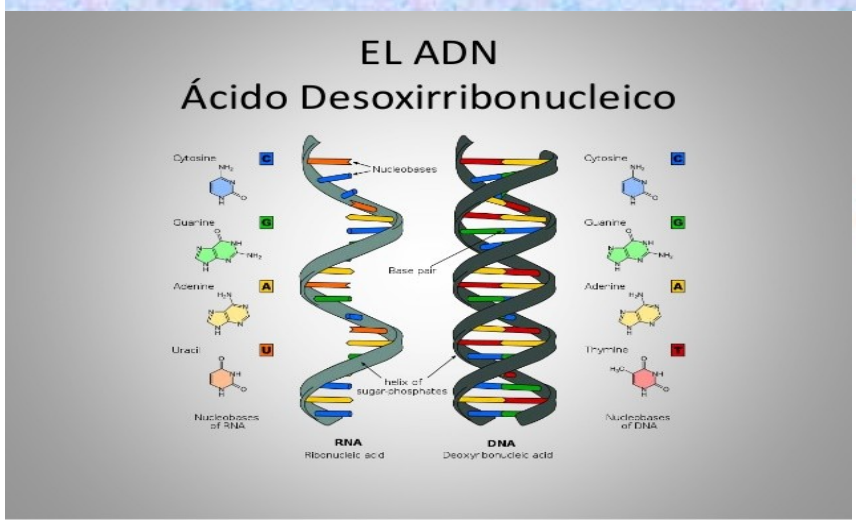
© Copyright Xavier Ribas 2017

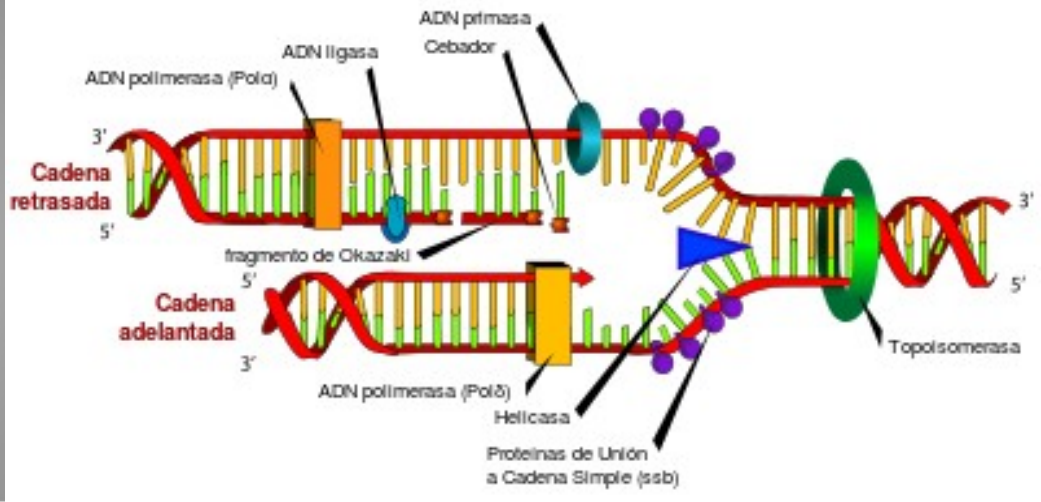
ribas 30 años 1987 - 2017

N D G
El Banco Nacional de Datos Genéticos es
el archivo público de material genético

DATOS GENÉTICOS

- 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**;



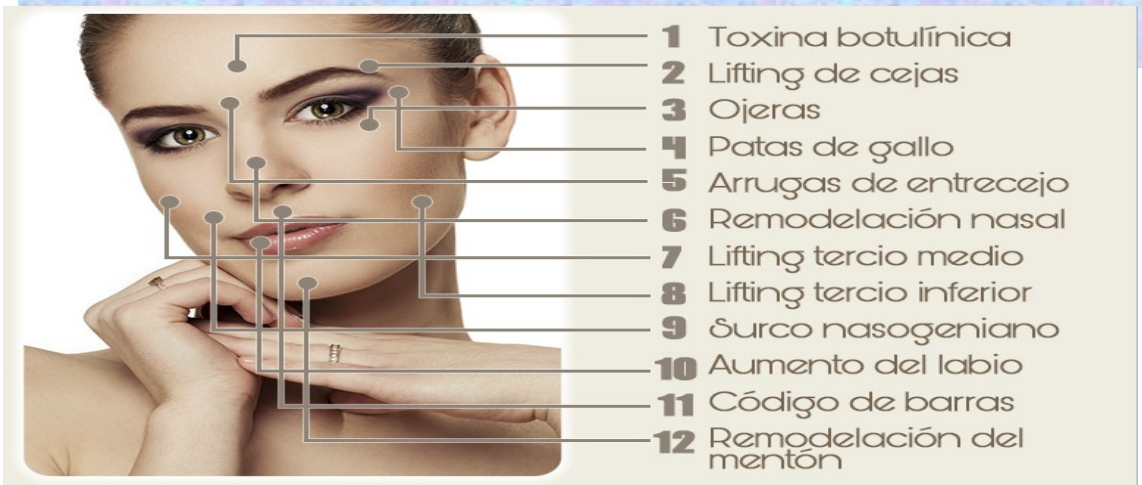


GDPR

¿Cómo se regula el tratamiento de **datos biométrico en la UE?**

DATOS BIOMÉTRICOS

- 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**;



MÉDICOS Y CLÍNICAS: CÓMO CUMPLIR EL RGPD

DATOS RELATIVOS A LA SALUD

- **DATOS PERSONALES RELATIVOS A LA SALUD FÍSICA O MENTAL DE UNA PERSONA FÍSICA**, incluida la **prestación de servicios de atención sanitaria**, que revelen información sobre su estado de salud.

ESTABLECIMIENTO PRINCIPAL

- El LUGAR DE **SU ADMINISTRACIÓN CENTRAL EN LA UNIÓN EUROPEA**, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión, y este **último establecimiento** tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considera **establecimiento principal.**

REPRESENTANTE

- **RESPONSABLE DEL TRATAMIENTO CON ESTABLECIMIENTOS EN MÁS DE UN ESTADO MIEMBRO**: el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considera establecimiento principal;

REPRESENTANTE

- **ENCARGADO DEL TRATAMIENTO CON ESTABLECIMIENTOS EN MÁS DE UN ESTADO MIEMBRO:** el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al **Reglamento.**

EMPRESA

- **Persona física o jurídica establecida en la Unión** que, habiendo sido designada por escrito por **el responsable o el encargado del tratamiento**, **represente al responsable o al encargado** en lo que respecta a sus **respectivas obligaciones** en virtud del **Reglamento PD.**

GRUPO EMPRESARIAL

- **Grupo constituido por una empresa** que ejerce el control y **sus empresas controladas**.

NORMAS CORPORATIVAS VINCULANTES

- Las **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.

Fases / partes del proceso:

- Normas internas en grupos internacionales
- Garantías en la protección de los datos
- Vinculación para todas las empresas del grupo
- Exigibles conforme a la norma española
- Autorización del director de la AEPD

Así debe ser un Plan de Cumplimiento del RGPD

PROCEDIMIENTOS

- Evaluaciones de Impacto de Privacidad (EIP)
- Notificación de Violaciones de Seguridad
- Ejercicio Derechos ARCOP
- Envío de Comunicaciones Comerciales
- Formación

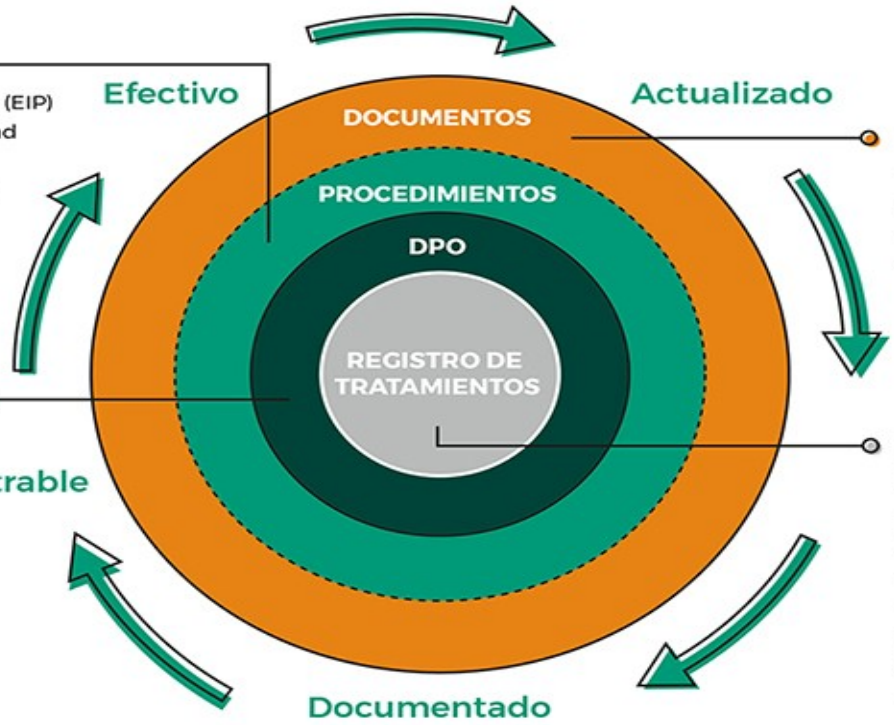
DPO (DATA PROTECTION OFFICER)

Perfil

Experiencia adecuada
Formación en legislación
Conocimiento sector
Conocimiento actividad

Funciones

Reuniones directivas
Recogida de información
Análisis y comprobación cumplimiento
Recomendaciones, consejos
Asistencia PIAs



DOCUMENTOS

- Cláusulas de información y consentimiento
- Política de Privacidad Web
- Acuerdo de Encargado de Tratamiento
- Política de Conservación de Datos (depuración y conservación)

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- Identificación del/os responsable/s
- Fines del tratamiento
- Categorías de interesados y de datos
- Categorías de destinatarios
- Transferencias internacionales
- Plazos de conservación
- Medidas técnicas y organizativas

GARRIGUES

AUTORIDAD DE CONTROL

- La **AUTORIDAD PÚBLICA INDEPENDIENTE** establecida por un Estado miembro para supervisar la aplicación del **Reglamento PD**, con el fin de **proteger los derechos y las libertades fundamentales de las personas físicas** en lo que respecta al tratamiento, y de facilitar la libre circulación de datos personales en la Unión.

LOS ÓRGANOS PÚBLICOS EUROPEOS QUE GESTIONAN LA PROTECCIÓN DE DATOS

EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

- Es organismo de la UE con personalidad jurídica que tiene como cometidos asesorar a la **Comisión Europea** en Protección de datos, elaborar directrices, recomendaciones y buenas prácticas. Está compuesto por el **Director de una autoridad de control de cada Estado miembro** y por el **Supervisor Europeo de Protección de Datos** o sus representantes respectivos

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS.

- Es un órgano independiente de la UE que tiene como objetivo principal garantizar que, a la hora de tratar datos personales, las instituciones y organismos de la UE respeten el derecho a la privacidad de los ciudadanos. Junto al **SUPERVISOR PRINCIPAL** existe un **SUPERVISOR ADJUNTO** que son elegidos para un mandato renovable de 5 años.
- Su web es: **https://edps.europa.eu/**

INFRACCIONES Y SANCIONES RGPD vs LOPD

AUTORIDAD DE CONTROL INTERESADA

La AUTORIDAD DE CONTROL A LA QUE AFECTA EL TRATAMIENTO DE DATOS PERSONALES debido a que:

- el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
- los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o
- se ha presentado una reclamación ante esa autoridad de control.

3 de julio / 15h00
Salón de uso Múltiple de
Sede Granados

y Tratamiento Transfronterizo
Datos Personales

Expositor: Joel Gómez Treviño

Contacto: Isabel Proaño /
isabel.proano@udla.edu.ec
Teléfono: 398-1000 ext: 2586

TRATAMIENTO TRANSFRONTERIZO

- **El tratamiento de datos personales** realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado **El tratamiento de datos personales** miembro, o
- realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

OBJECIÓN PERTINENTE Y MOTIVADA

- La objeción a una propuesta de decisión sobre la existencia o no de infracción del **Reglamento**, o sobre la conformidad con el **Reglamento** de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

SERVICIO DE LA SOCIEDAD DE LA INFORMACIÓN

- **Servicio de la sociedad de la información** es aquel que se presta a distancia, por vía electrónica, a petición individual del destinatario, y normalmente a cambio de una remuneración.
- En términos generales, estos servicios comprenden los prestados a través de Internet siempre que representen una actividad económica para el prestador.
- **Su régimen jurídico** se establece parcialmente en la **DIRECTIVA sobre el comercio electrónico** y en las disposiciones legales de los Estados Miembros de la Unión Europea que transponen esta Directiva.

LSSICE

LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y COMERCIO ELECTRÓNICO

ORGANIZACIÓN INTERNACIONAL

- Una **ORGANIZACIÓN INTERNACIONAL y sus entes subordinados de Derecho internacional público** o cualquier otro **organismo** creado mediante un **acuerdo entre dos o más países** o en virtud de tal acuerdo.

PRINCIPIOS DE PROTECCIÓN DE DATOS

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

PRINCIPIOS DE PROTECCIÓN DE DATOS

Legalidad	Finalidad	Libertad	Veracidad
Transparencia	Acceso y regulación restringida	Seguridad	Confidencialidad

PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS

¿FUNDAMENTOS Y/O DEBERES?

- Los **PRINCIPIOS GENERALES DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**, no sólo son meros fundamentos por los que se ha de regir la elaboración, interpretación y aplicación de la normativa sobre protección de datos, sino que se trata de un conjunto de reglas que determinan cómo recoger, tratar y ceder los datos.
- En caso de encontrarnos con **lagunas o vacíos legales**, nos hemos de inspirar en éstos, para que el tratamiento de los datos sea conforme a la normativa.
- En definitiva, son **deberes y obligaciones a los que están sujetos los tratamientos de datos de carácter personal.**

PRINCIPIOS DE PROTECCIÓN DE DATOS

Recogidos en el **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA**

LEALTAD – No pueden recabarse datos personales por medios fraudulentos (esto es, no pueden utilizase medios o métodos engañosos) **desleales** (que den lugar a una discriminación injusta o arbitraria contra los titulares) **e ilícitos** (es decir, que sean ilegales, estén fuera o al margen de la Ley).

PRINCIPIOS DE PROTECCIÓN DE DATOS

- **TRANSPARENCIA –** Exige que toda información y comunicación relativa al tratamiento de datos personales sea **fácilmente accesible y fácil de entender**, y que **se utilice un lenguaje sencillo y claro**.

PRINCIPIOS DE PROTECCIÓN DE DATOS

LICITUD O LEGITIMACIÓN DEL TRATAMIENTO.-Para que el tratamiento sea lícito, los datos personales deben ser tratados con el **consentimiento explícito del interesado** o sobre otra base o fundamento jurídico **(artículo 6 RGPD).**

Informe AEPD sobre legitimación para el tratamiento de datos de salud

Legitimación

Art. 6.1

a) consentimiento para el tratamiento de sus datos personales para uno o más fines específicos

b) ejecución de un contrato en el que el interesado es parte o para la aplicación, a petición de éste, de medidas precontractuales

c) cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento

d) intereses vitales del interesado o de otra persona física

e) cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los interés o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones

PRINCIPIOS DE PROTECCIÓN DE DATOS

- **LIMITACIÓN DE LA FINALIDAD.-** Los datos personales deben ser recogidos con **fines determinados, explícitos y legítimos**, y no serán tratados, posteriormente, **de manera incompatible o distinta con dichos fines.**

PRINCIPIOS DE PROTECCIÓN DE DATOS

MINIMIZACIÓN.- Deben ser **adecuados, pertinentes y limitados o no excesivos**, en relación con los **fines que legitiman el tratamiento.**

PRINCIPIOS DE PROTECCIÓN DE DATOS

- **EXACTITUD-** Los **datos deben ser exactos** y, si fuera necesario, **actualizados**. Deben **ADOPTARSE TODAS LAS MEDIDAS RAZONABLES** para **corregir errores, modificar los datos que resulten ser inexactos o incompletos** y garantizar la certeza de la información objeto de tratamiento.

PRINCIPIOS DE PROTECCIÓN DE DATOS

LIMITACIÓN DEL PLAZO DE CONSERVACIÓN.-

- No pueden conservarse o mantenerse los datos durante más tiempo del necesario para los fines del tratamiento.
- Deben establecerse plazos para la supresión o revisión periódica.

PRINCIPIOS DE PROTECCIÓN DE DATOS

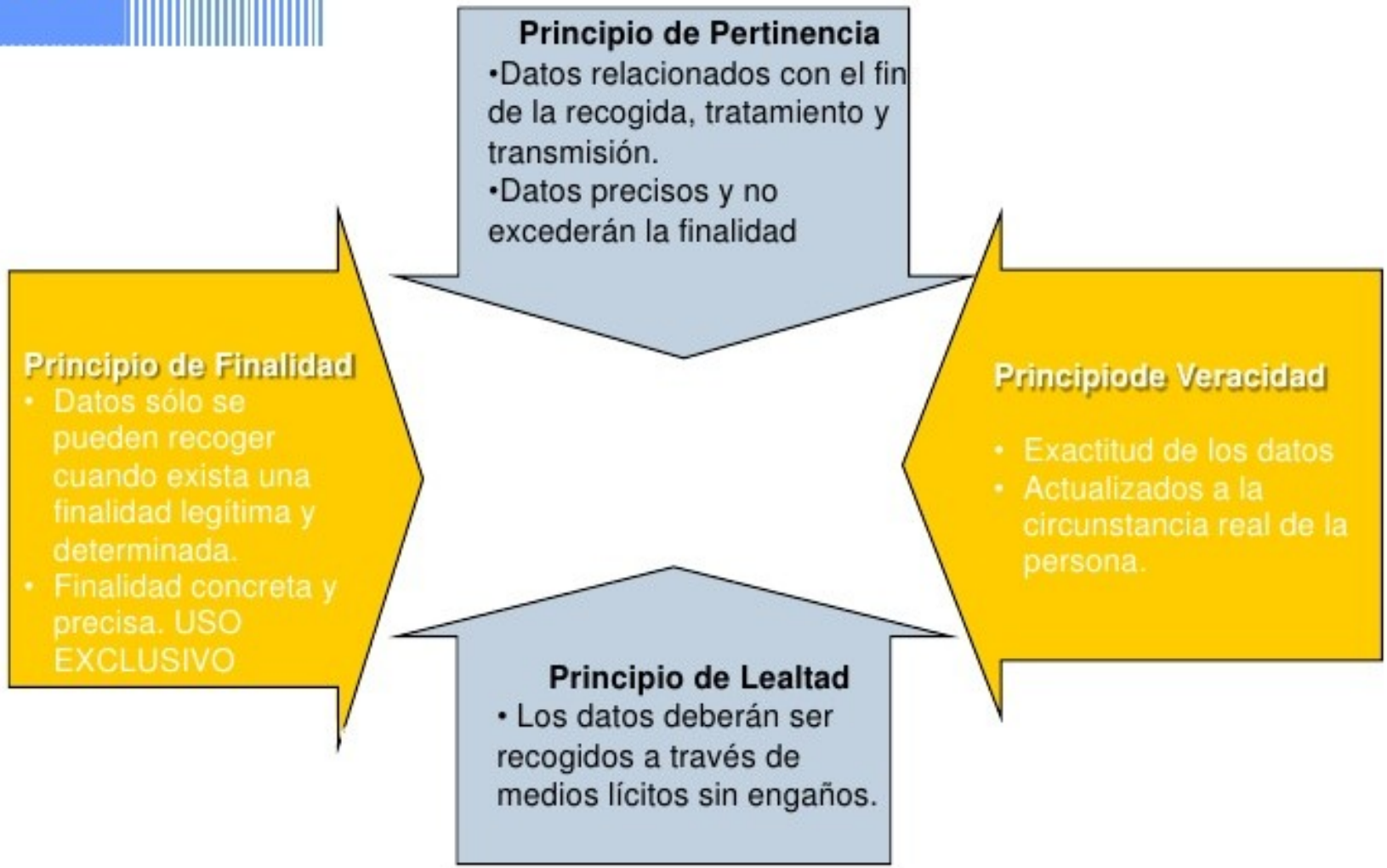
- **INTEGRIDAD Y CONFIDENCIALIDAD.-**

❑ Debe **garantizarse una seguridad adecuada** para preservar la integridad de los datos e impedir el acceso o uso no autorizado.

❑ Todas las personas que intervengan en cualquier fase del tratamiento están **sujetas a guardar SECRETO O CONFIDENCIALIDAD** con carácter indefinido.

Confidencialidad de los datos personales

El tratamiento de Datos Personales debe contemplar "Principio de Calidad"



EXACTITUD DE LOS DATOS

PINTOS & SALGADO
ABOGADOS

Principio de Exactitud (calidad)

- Los datos de carácter personal serán **exactos y puestos al día** de forma que respondan con veracidad a la situación actual del afectado.
- Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán **cancelados y sustituidos de oficio** por los correspondientes datos rectificados o completados.
  - Ello sin perjuicio de los derechos A.R.C.O.

Copyright © Pintos & Salgado, 2016

Cómo deben tratarse los datos

La calidad de los datos

Pertinentes

Adecuados

No excesivos

- Insertar sólo los datos necesarios
- Los datos no se podrán utilizar para otra finalidad distinta a la que se requirió
- Exactitud de los datos personales
- Cancelar los datos cuando dejen de ser necesarios
- Conservar los datos que por razones legales sean necesarios
- Almacenar los datos de forma que facilite el derecho de acceso
- Se prohíbe la recogida de datos por medios fraudulentos o ilícitos

EXACTITUD DE LOS DATOS

REGLA GENERAL:

- Los datos serán **EXACTOS** y, si fuere 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**

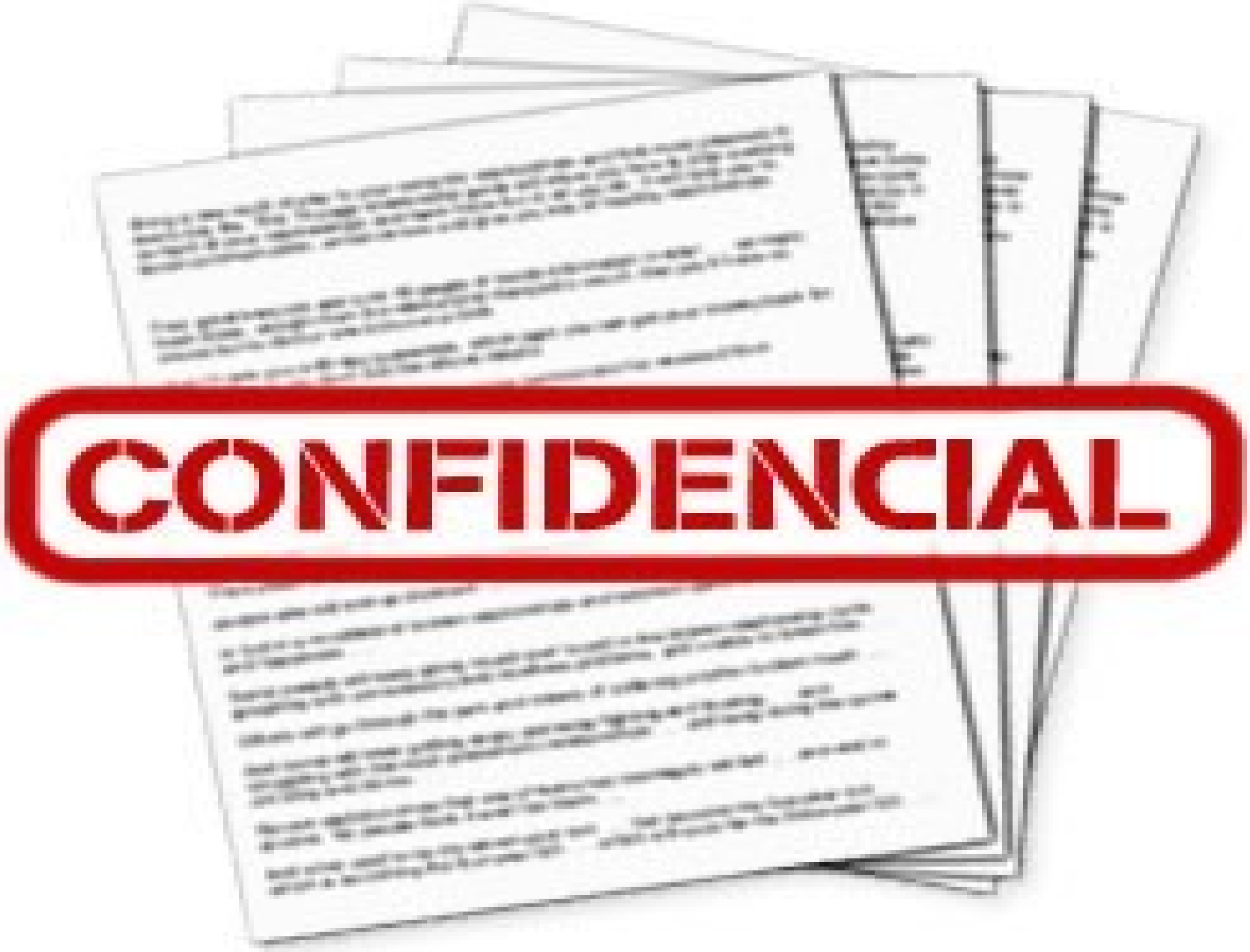
EXACTITUD DE LOS DATOS

- El **PRINCIPIO DE EXACTITUD DE LOS DATOS** determina a su vez la necesidad de articular procedimientos que permitan al responsable **realizar la actualización continua de los datos contenidos en el fichero** con la finalidad de respetar el citado principio, de tal manera que sean exactos y se ajusten a la realidad del interesado.
- Estos datos **se tratarán de modo leal**, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley

EXACTITUD DE LOS DATOS

La inexactitud de los datos personales no es imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, con respecto a los fines para los que se tratan, cuando los datos inexactos:

- Hubiesen sido obtenidos por el responsable directamente del afectado.
- Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. **El mediador o intermediario** asume las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.
- Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad.
- Fuesen obtenidos de un registro público por el responsable.


CONFIDENCIAL

DEBER DE CONFIDENCIALIDAD

- Los **RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO** de datos así como todas las personas que intervengan en cualquier fase de este están sujetas al **DEBER DE CONFIDENCIALIDAD**.
- La obligación general anterior es complementaria de los **DEBERES DE SECRETO PROFESIONAL** de conformidad con su normativa aplicable.
- Las **obligaciones anteriores** se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

SECRETO PROFESIONAL

El secreto profesional es la obligación legal que tienen ciertas profesiones de mantener en secreto la información que han recibido de sus clientes. Al contrario de lo que ocurre con tipos de deberes de confidencialidad, el secreto profesional se mantiene incluso en un juicio.

Entre estos profesionales, cabe citar como casos más típicos el abogado, el médico, el enfermero, el psicólogo, el periodista el trabajador social. Sin embargo, también puede haber otros casos de asesores o servicios que tengan ese tipo de obligación, por ejemplo los asesores fiscales

CONSENTIMIENTO RGPD

- LIBRE
- ESPECÍFICO
- INFORMADO
- INEQUÍVOCO

CARACTERÍSTICAS

- DEMOSTRACIÓN
- DISTINCIÓN
- REVOCACIÓN
- LIBERTAD

CONDICIONES

TRATAMIENTO BASADO EN EL CONSENTIMIENTO DEL AFECTADO

- **CONSENTIMIENTO DEL AFECTADO** es toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- Cuando se pretenda fundar el tratamiento de los datos en el **CONSENTIMIENTO DEL AFECTADO** para una pluralidad de finalidades es preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.
- No puede supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden **relación con el mantenimiento, desarrollo o control de la relación contractual.**

CONSENTIMIENTO DE LOS MENORES DE EDAD

- El **tratamiento de los datos personales de un menor de edad** únicamente puede fundarse en su consentimiento cuando sea mayor de 14 años.
- Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.
- El **TRATAMIENTO DE LOS DATOS DE LOS MENORES DE 14 AÑOS,** fundado en el consentimiento, solo es lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

TRATAMIENTO DE DATOS POR OBLIGACIÓN LEGAL, INTERÉS PÚBLICO O EJERCICIO DE PODERES PÚBLICOS

- El **tratamiento de datos personales** solo puede considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que puede determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal.
- Dicha norma puede igualmente imponer condiciones especiales al tratamiento, tales como **la adopción de medidas adicionales de seguridad.**
- El **tratamiento de datos personales** solo puede considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, cuando derive de una competencia atribuida por una norma con rango de ley.

CATEGORÍAS ESPECIALES DE DATOS

- A fin de evitar situaciones discriminatorias, el **solo consentimiento del afectado** no basta para levantar la prohibición del tratamiento de datos cuya **finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.**
- Lo anterior no impide el tratamiento de dichos datos cuando así proceda.
- Los tratamientos de datos contemplados en el Reglamento (UE) 2016/679 fundados en el Derecho español deben estar amparados en una **norma con rango de ley**, que puede establecer requisitos adicionales relativos a su seguridad y confidencialidad.
- En particular, dicha norma puede amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y **servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro** del que el afectado sea parte.

TRATAMIENTO DE DATOS DE NATURALEZA PENAL

- El **tratamiento de datos personales relativos a condenas e infracciones penales**, así como a **procedimientos y medidas cautelares y de seguridad conexas**, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo puede llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en la ley orgánica o en otras normas de rango legal.
- El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, podrá realizarse conforme con lo establecido en la regulación del **SISTEMA DE REGISTROS ADMINISTRATIVOS DE APOYO A LA ADMINISTRACIÓN DE JUSTICIA.**
- Fuera de los supuestos anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo son posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

DERECHOS DE LAS PERSONAS

DERECHOS DE LAS PERSONAS

TRANSPARENCIA E INFORMACIÓN AL AFECTADO.

Cuando **los DATOS PERSONALES SEAN OBTENIDOS DEL AFECTADO**, el **RESPONSABLE DEL TRATAMIENTO** puede dar cumplimiento al deber de información establecido en el RPD facilitando al afectado la información básica, e indicándole **una dirección electrónica** u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

LA INFORMACIÓN BÁSICA ANTERIOR debe contener, al menos:

- La identidad del responsable del tratamiento y de su representante, en su caso.
- La finalidad del tratamiento.
- La posibilidad de ejercer los derechos establecidos en el RPD.

- Si los **datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles**, la información básica comprenderá asimismo esta circunstancia.
- En este caso, **el afectado** debe ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho.

TRANSPARENCIA E INFORMACIÓN AL AFECTADO

- Cuando **los DATOS PERSONALES NO HUBIERAN SIDO OBTENIDOS DEL AFECTADO**, el responsable puede dar cumplimiento al deber de información establecido en el RPD facilitando a aquel la información básica anterior, indicándole una **dirección electrónica** u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
- En estos supuestos, la información básica incluirá también:
  - ❑ Las categorías de datos objeto de tratamiento.
  - ❑ Las fuentes de las que procedieran los datos.

EJERCICIO DE LOS DERECHOS

DISPOSICIONES GENERALES SOBRE EJERCICIO DE LOS DERECHOS.

- Los derechos reconocidos en el RPD pueden ejercerse directamente o por medio de representante legal o voluntario.
- El **responsable del tratamiento** está obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deben ser fácilmente accesibles para el afectado.
- El ejercicio del derecho no puede ser denegado por el solo motivo de optar el afectado por otro medio.

DISPOSICIONES GENERALES SOBRE EJERCICIO DE LOS DERECHOS.

- **El encargado** puede tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.
- La prueba del cumplimiento del deber de responder a la solicitud de ejercicio **del responsable.** sus derechos formulado por el afectado recae sobre
- En cualquier caso, **los titulares de la patria potestad** pueden ejercitar en nombre y representación de los menores de 14 años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.
- **Son gratuitas** las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos.

Derechos ARCO

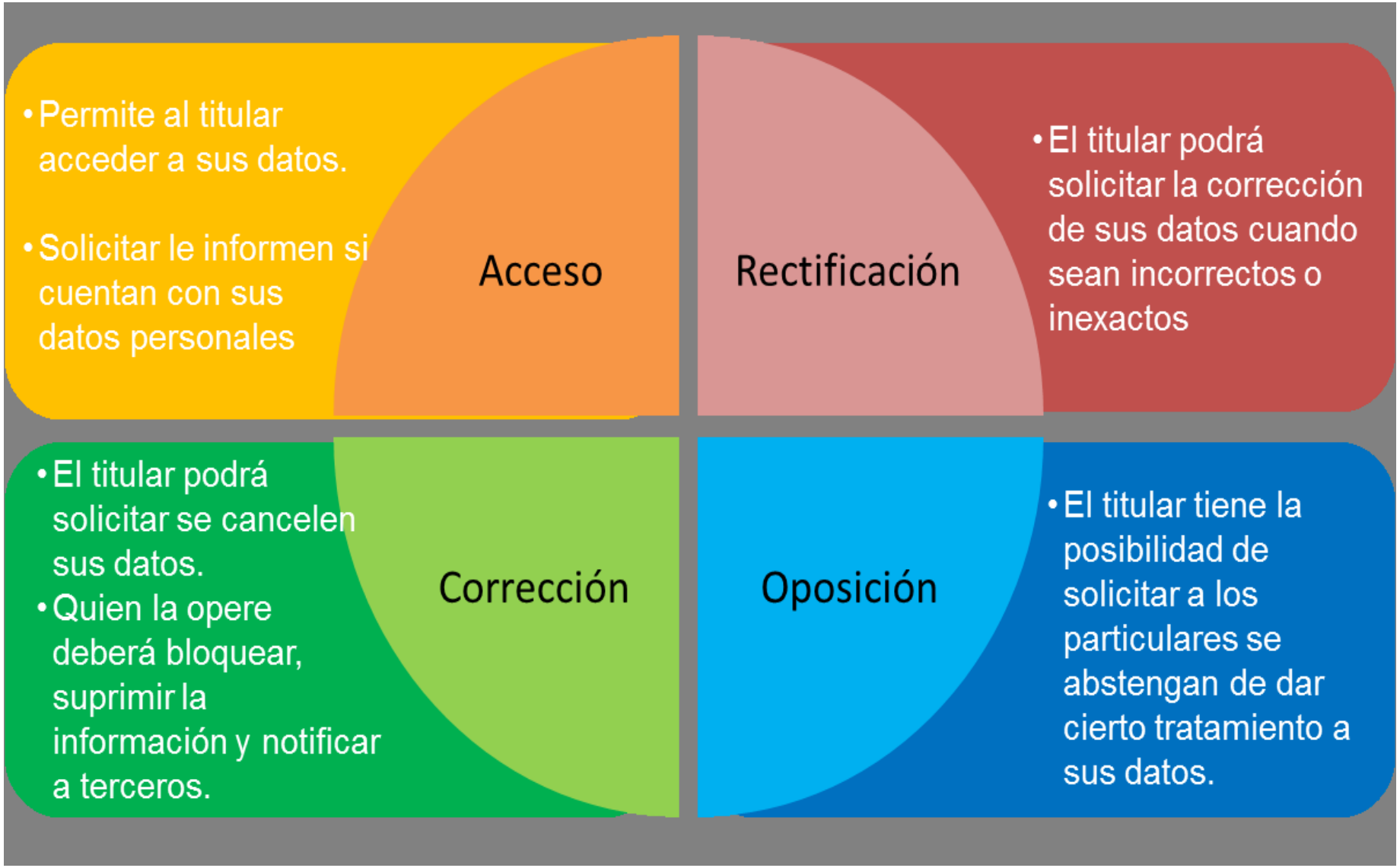
Acceso

Rectificación

Cancelación

Oposición

DERECHOS ARCO PROTECCION DATOS



LOPD
ACCESO
RECTIFICACIÓN
CANCELACIÓN
OPOSICIÓN
AMPLIACIÓN
DERECHOS
ARCO
RGPD
PORTABILIDAD
DATOS
OLVIDO

DERECHOS DEL CIUDADANO EN PROTECCIÓN DE DATOS

NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS
25 DE MAYO

Derecho al ACCESO

Para saber:

- Para que usan tus datos
- Quién los tiene y/o si han sido cedidos a terceros
- Plazos de conservación
- Derecho a reclamar ante la AGPD
- Existencias de decisiones automatizadas, elaborción de perfiles y consecuencias

Dereho a la RECTIFICACIÓN

- Datos inexactos
- Datos incompletos

Derecho a la SUPRESIÓN y LIMITACIÓN

- Por tratamiento ilícito
- Cambio de finalidad de tus datos
- Por oposición
- Revocación de consentimiento

Derecho a la OPOSICIÓN

- Motivos personales salvo que la entidad acredite un interés legítimo

*Cuando el tratamiento sea debido al MARKETING DIRECTO

Derecho a SOLICITAR INFORMACIÓN

La suspensión del tratamiento de tus datos
- Si impugnamos la exactitud de los datos, mientras se verifican
- Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos son legítimos

La conservación de tus datos
- Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso
- Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones

La portabilidad de tus datos a terceros
- En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato

Derechos de los interesados

Cualquier tratamiento

- Acceso
- Rectificación
- Supresión
- Limitación
- Oposición

Tratamiento automatizado

- Portabilidad
- Oponerse a la elaboración de perfiles

Otros derechos

- Revocación del consentimiento
- Reclamación a la Autoridad de control

ACCESO

DERECHO DE ACCESO del INTERESADO

El interesado tiene **DERECHO A OBTENER DEL RESPONSABLE DEL TRATAMIENTO CONFIRMACIÓN DE SI SE ESTÁN TRATANDO O NO DATOS PERSONALES QUE LE CONCIERNEN** y, en tal caso, **DERECHO DE ACCESO A LOS DATOS PERSONALES** y a la siguiente **INFORMACIÓN:**

- los fines del tratamiento;
- las categorías de datos personales de que se trate;
- los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
- de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- el **derecho a presentar una reclamación ante una autoridad de control;**
- cuando los datos personales no se hayan obtenido del interesado, cualquier **información disponible sobre su origen**;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

DERECHO DE ACCESO del INTERESADO

- Cuando se **transfieran datos personales a un tercer país o a una organización internacional,** el interesado tiene derecho a ser informado de las garantías adecuadas relativas a la transferencia.
- El responsable del tratamiento debe facilitar una copia de los datos personales objeto de tratamiento.
- El responsable puede percibir por cualquier otra copia solicitada por el interesado **un canon razonable** basado en los costes administrativos.
- Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilita en un formato electrónico de uso común.
- El derecho a obtener copia no afectará negativamente a los derechos y libertades de otros.

DERECHO DE ACCESO del INTERESADO

- Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable puede solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.
- El **DERECHO DE ACCESO** se entiende otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad.
- A tales efectos, la comunicación por el responsable al afectado del modo en que este pueda acceder a dicho sistema basta para tener por atendida la solicitud de ejercicio del derecho.
- Se puede considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante **el plazo de seis meses**, a menos que exista causa legítima para ello.
- Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud se considera **excesiva**, por lo que dicho afectado asumirá el exceso de costes que su elección comporte.
- En este caso, solo es exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

A. DERECHO DE ACCESO.

A.1. EJERCICIO DEL DERECHO DE ACCESO[1].

DATOS DEL RESPONSABLE DEL FICHERO[2].

Nombre / razón social: .....
Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso:
C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....
C.I.F./D.N.I. .....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL[3].

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 12 y 13 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Segunda de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En .....a.....de.....de 20.....

Firmado:

---

1 Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos.

2 Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

3 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

R
RECTIFICACIÓN

DERECHO DE RECTIFICACIÓN

- El interesado tiene derecho a obtener sin dilación indebida del responsable del tratamiento **la RECTIFICACIÓN DE LOS DATOS PERSONALES INEXACTOS que le conciernan**.
- Teniendo en cuenta los fines del tratamiento, el interesado tiene derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.
- Al ejercer el **derecho de rectificación**, el afectado debe indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse.
- Debe acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

CANCELACIÓN

DERECHO DE SUPRESIÓN
EL DERECHO AL OLVIDO

El interesado tiene **DERECHO A OBTENER SIN DILACIÓN INDEBIDA DEL RESPONSABLE DEL TRATAMIENTO LA SUPRESIÓN DE LOS DATOS PERSONALES QUE LE CONCIERNAN**, el cual está obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de **las circunstancias siguientes**:

- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- el interesado retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico;
- el interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento.
- los datos personales hayan sido tratados ilícitamente;
- los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Cuando la supresión derive del ejercicio del derecho de oposición el responsable puede conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

DERECHO DE SUPRESIÓN

Cuando haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, debe adoptar medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

- Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

❑para ejercer el derecho a la libertad de expresión e información;

❑para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

❑por razones de interés público en el ámbito de la salud pública.

❑con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

❑para la formulación, el ejercicio o la defensa de reclamaciones.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO.

El interesado tiene derecho a obtener del responsable del tratamiento la **LIMITACIÓN DEL TRATAMIENTO DE LOS DATOS** cuando se cumpla alguna de las condiciones siguientes:

- ❑el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
- ❑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, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
- ❑el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

- El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

- Cuando el tratamiento de datos personales se haya **LIMITADO**, dichos datos solo pueden ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.
- Todo interesado que haya obtenido **LA LIMITACIÓN DEL TRATAMIENTO** será informado por el responsable antes del levantamiento de dicha limitación.

OBLIGACIÓN DE NOTIFICACIÓN RELATIVA A LA RECTIFICACIÓN O SUPRESIÓN DE DATOS PERSONALES O LA LIMITACIÓN DEL TRATAMIENTO

- El **RESPONSABLE DEL TRATAMIENTO** debe comunicar cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.
- El **RESPONSABLE** debe informar al interesado acerca de dichos destinatarios, si este así lo solicita.

REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

PORTABILIDAD DE DATOS

DERECHO A LA PORTABILIDAD

- El interesado tiene derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

❑ el tratamiento esté basado en el consentimiento, o en un contrato, y

❑ el tratamiento se efectúe por medios automatizados.

- Al ejercer su derecho a la portabilidad de los datos, el interesado tiene derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
- El ejercicio del derecho se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- El derecho no debe afectar negativamente a los derechos y libertades de otros.

LOPD
tugest

DERECHO DE OPOSICIÓN

- El interesado tiene **DERECHO A OPONERSE** en cualquier momento, **por motivos relacionados con su situación particular**, a que datos personales que le conciernan sean objeto de un tratamiento, incluida **la elaboración de perfiles** sobre la base de dichas disposiciones.
- El **RESPONSABLE DEL TRATAMIENTO** **dejará de tratar los datos personales,** salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

DERECHO DE OPOSICIÓN

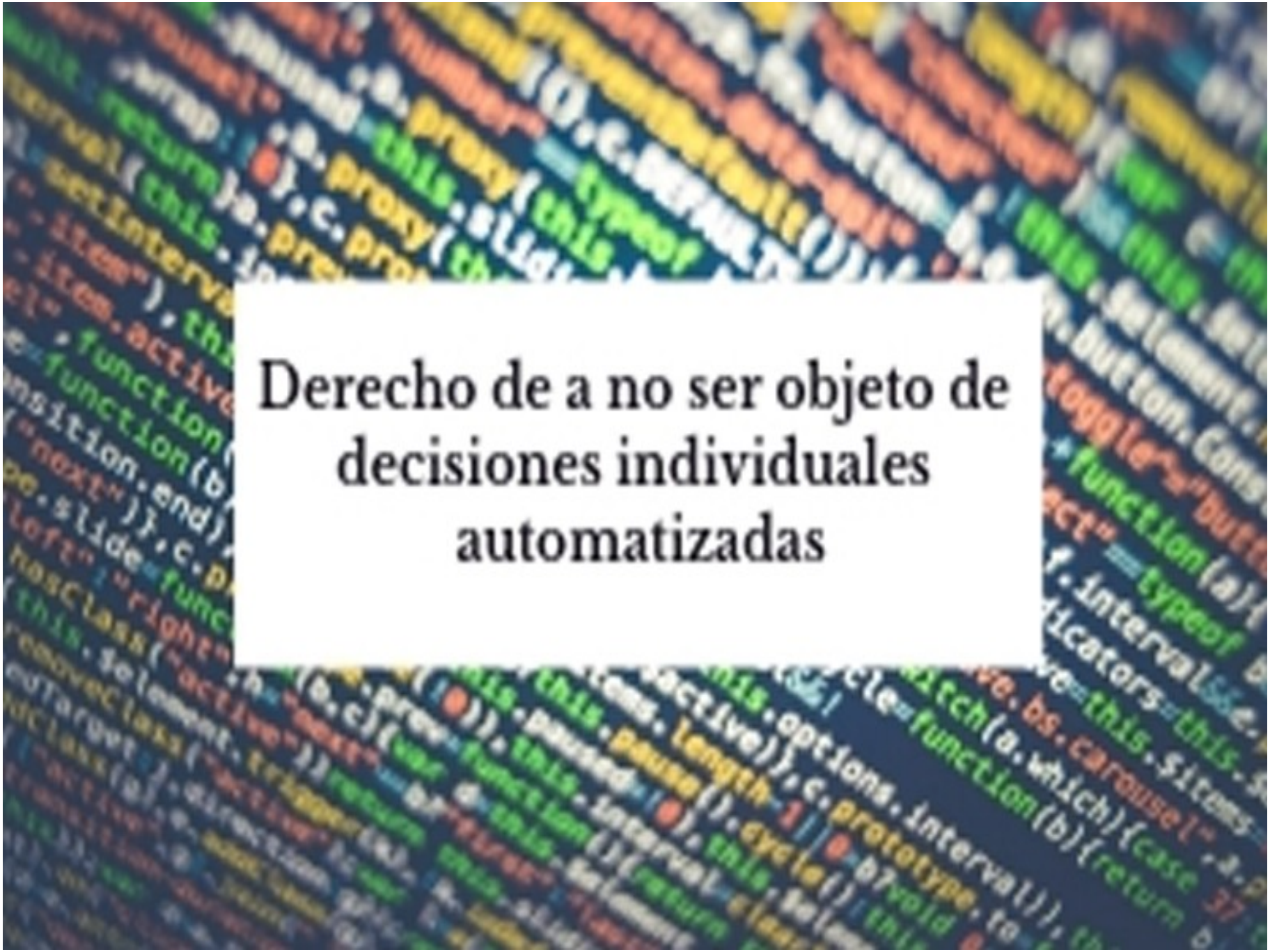
- **LA MERCADOTECNIA DIRECTA O MARKETING DIRECTO** es una forma de publicidad que utiliza uno o más medios para comunicarse directamente con un público objetivo y obtener de él una respuesta medible.

DERECHO DE OPOSICIÓN

- Cuando el **tratamiento de datos personales** tenga por objeto **LA MERCADOTECNIA DIRECTA**, el interesado tiene derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida **la elaboración de perfiles** en la medida en que esté relacionada con la citada **mercadotecnia.**
- Cuando **el interesado se oponga al tratamiento con fines de mercadotecnia directa**, los datos personales dejarán de ser tratados para dichos fines.
- A más tardar, en el momento de **la primera comunicación con el interesado**, **este derecho será mencionado explícitamente al interesado.** y será presentado claramente y al margen de cualquier otra información.

DERECHO DE OPOSICIÓN

- En el contexto de **la utilización de servicios de la sociedad de la información**, el interesado puede ejercer **su derecho a oponerse por medios automatizados** que apliquen especificaciones técnicas.
- Cuando **los datos personales se traten con FINES DE INVESTIGACIÓN CIENTÍFICA O HISTÓRICA O FINES ESTADÍSTICOS**, el interesado tiene derecho, por motivos relacionados con su situación particular, a **oponerse al tratamiento de datos personales que le conciernan,** salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.


Derecho de a no ser objeto de decisiones individuales automatizadas

DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES

- **Todo INTERESADO** tiene **DERECHO A NO SER OBJETO DE UNA DECISIÓN BASADA ÚNICAMENTE EN EL TRATAMIENTO AUTOMATIZADO**, incluida **LA ELABORACIÓN DE PERFILES**, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

DIFERENCIA ENTRE AMBOS CONCEPTOS.

- **DECISIONES INDIVIDUALES AUTOMATIZADAS:** la habilidad de tomar **decisiones por medios tecnológicos** sin intervención humana.
- **ELABORACIÓN DE PERFILES: la recogida de datos sobre un individuo,** y el **análisis de sus características o patrones de comportamiento** para categorizarles o realizar predicciones o afirmaciones sobre su capacidad para realizar una tarea, sus intereses o su comportamiento probable.

ELABORACIÓN DE PERFILES

- Se considera que **SE ELABORAN PERFILES** cuando sus aspectos personales son evaluados para elaborar predicciones sobre su persona, incluso si no se toman decisiones.
- **Por ejemplo**, si una empresa u organización evalúa sus características (como la edad, el sexo, la altura) o le incluye en una categoría, significa que **SE ESTÁ ELABORANDO UN PERFIL SOBRE LAS PERSONAS.**

ELABORACIÓN DE PERFILES

- La **elaboración de perfiles y las decisiones automatizadas** son práctica habitual en muchos sectores, como **el bancario y financiero, el fiscal y la sanidad.**
- Puede ser más eficiente, pero es menos transparente y puede limitar su elección.

ELABORACIÓN DE PERFILES

- Si utilizamos **un banco por internet** para un préstamo.
- Nos piden que introduzcamos nuestros datos, y el algoritmo del banco le dice si el banco nos concederá el préstamo o no, y nos sugiere un tipo de interés.
- Se nos debe **INFORMAR** de que puede expresar su opinión, impugnar la decisión y solicitar la contribución de una persona en el proceso para revisar la decisión tomada mediante el algoritmo.

EXCEPCIONES AL DERECHO

ESTE DERECHO NO SE APLICA si la decisión:

- ❑es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
- ❑está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
- ❑se basa en el consentimiento explícito del interesado.

- En estos casos, **EL RESPONSABLE DEL TRATAMIENTO** adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo **el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.**

DERECHOS.

- El **GT29** establece que **LOS RESPONSABLES deben ser especialmente conscientes de sus obligaciones de transparencia ya que el proceso de elaboración de perfiles es a menudo invisible para los interesados.**

DICTAMEN SOBRE LA TOMA DE DECISIONES INDIVIDUALES AUTOMATIZADAS Y LA ELABORACIÓN DE PERFILES DEL GT 29

- **DISPOSICIONES GENERALES SOBRE ELABORACIÓN DE PERFILES Y TOMA DE DECISIONES AUTOMÁTICA**. El GT29 proporciona una visión general de las disposiciones aplicadas tanto a la elaboración de perfiles como a la toma automatizada de decisiones. Para ayudar al cumplimiento, el GT29 establece que los responsables deben considerar las siguientes **ÁREAS CLAVE:**

❑**TRANSPARENCIA DEL PROCESO DE ELABORACIÓN DE PERFILES**. El proceso de elaboración de perfiles implica la creación de "nuevos" datos personales derivados o deducidos sobre los sujetos de datos, que ellos mismos no han proporcionado directamente.

❑**Compatibilidad del tratamiento adicional con el la finalidad original para el que se recopilaron los datos.**

❑**Minimización de datos y capacidad de explicar y justificar la necesidad de recopilar y mantener los datos personales**. Los responsables deben considerar exactitud en todas las etapas de la elaboración de perfiles, específicamente cuando recojan y analicen datos, creen un perfil para un individuo o apliquen un perfil para tomar decisiones que le afectan.

❑**Limitación de almacenamiento**, porque el almacenamiento de información a largo plazo puede entrar en conflicto con la proporcionalidad.

TRATAMIENTO DE DATOS DE CONTACTO, DE EMPRESARIOS INDIVIDUALES Y DE PROFESIONALES LIBERALES.

- Salvo prueba en contrario, se presume amparado en el Reglamento (UE) el **TRATAMIENTO DE LOS DATOS DE CONTACTO Y EN SU CASO LOS RELATIVOS A LA FUNCIÓN O PUESTO DESEMPEÑADO DE LAS PERSONAS FÍSICAS QUE PRESTEN SERVICIOS EN UNA PERSONA JURÍDICA** siempre que se cumplan los siguientes requisitos:

❑Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

❑Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

- La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.
- Los responsables o encargados del tratamiento podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Sistema de Información Crediticia

Un sistema de fiar a su servicio...

- **QUÉ ES UN SISTEMA DE INFORMACIÓN CREDITICIA**
- **ENCONTRARSE INCLUIDO EN UNO DE ESTOS SISTEMAS PUEDE LIMITAR MUCHO NUESTRA CAPACIDAD DE ACCEDER A FINANCIACIÓN.**
- **REGISTRO DE MOROSOS.**
- SISTEMAS DE SOLVENCIA PATRIMONIAL

Ficheros de Morosos

LOS SISTEMAS DE INFORMACIÓN CREDITICIA BAJO EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

- Un **SISTEMA DE INFORMACIÓN CREDITICIA** es un sistema en el que se incluyen a todas aquellas personas físicas o jurídicas que **hayan incurrido en algún tipo de impago.**
- Bajo esta definición se esconde un amplio abanico de formas de acabar en **uno de estos sistemas que perjudican enormemente a quien figura en ellos ya que restringe de manera notable su acceso a cualquier tipo de financiación.**

LOS SISTEMAS DE INFORMACIÓN CREDITICIA BAJO EL RGPD

- Estos sistemas se utilizan en España como **una herramienta de información** para multitud de empresas, entre ellas **las entidades financieras**, que necesitan conocer el historial o situación de pagos de sus clientes.
- Existen varios sistemas de información crediticia en la actualidad: Uno de las más importantes es el de **ASNEF** que gestiona **ASNEF-EQUIFAX SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA Y CRÉDITO S.L.**; otro de los sistemas más consultados por las empresas es el que lleva el **Registro de Aceptaciones Impagadas**, conocido por su acrónimo, **RAI.**
- Por último, otro de los sistemas más conocidos es el **BADEXCUG**, que gestiona la empresa **EXPERIAN BUREAU DE CREDITO, S.A.**

REQUISITOS DE INCLUSIÓN EN UN SISTEMA DE INFORMACIÓN CREDITICIA

- Cuando uno piensa en un sistema de información crediticia cree que ahí solo se reflejan los nombres de los grandes deudores, personas que no han tenido cuidado con sus finanzas y ahora deben ingentes cantidades de dinero a numerosos acreedores.
- En realidad no es así y para acabar en uno de estos sistemas no se necesita ni tener una deuda elevada ni contar con numerosos acreedores.
- En España los **SISTEMAS DE INFORMACIÓN CREDITICIA** están regulados por la **Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales**.
- Al final, nuestra información patrimonial y financiera es un bien más que debemos cuidar.

REQUISITOS DE INCLUSIÓN EN UN SISTEMA DE INFORMACIÓN CREDITICIA

Se presume lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan **los siguientes requisitos:**

- Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.
- Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.
- Que el acreedor haya informado al afectado en el contrato o en el momento de requerirle el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe. La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito debe notificar al afectado la inclusión de tales datos, y le informará sobre la posibilidad de ejercitar los derechos establecidos en **el Reglamento (UE) 2016/679** dentro de los treinta (30) días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

REQUISITOS DE INCLUSIÓN EN UN SISTEMA DE INFORMACIÓN CREDITICIA

- Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con **el límite máximo de cinco (5) años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.**
- Que los datos referidos a un deudor determinado solamente pueden ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario
- Que, en el caso de que se denegase la solicitud de celebración del contrato, o este no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.
- **Que las deudas incluidas en dichos sistemas no sean inferiores a 50 euros. El Gobierno, mediante Real Decreto**, podrá actualizar esta cuantía.

¿QUÉ CONSECUENCIAS TIENE ESTAR EN UN SISTEMA DE INFORMACIÓN CREDITICIA?

- Cuando somos incluidos en **UN SISTEMA DE INFORMACIÓN CREDITICIA** nuestras posibilidades para acceder a préstamos y créditos (en definitiva, a financiación bancaria), se verán reducidas de manera radical.
- A partir de entonces **los bancos y otras entidades que ofrecen crédito** recelarán de nuestra capacidad de pagar deudas y, por tanto, en pocas ocasiones, por no decir ninguna, nos concederán dinero o crédito.

¿CÓMO SE SALE DE UN SISTEMA DE INFORMACIÓN CREDITICIA?

- Para salir de **UN SISTEMA DE INFORMACIÓN CREDITICIA** hay que saldar la deuda que nos exigen y por la cual nos han incluido en uno de estos sistemas.
- Una vez realizado el pago, la gestora del sistema debe eliminar los datos en un plazo máximo de un mes, eso sí, antes consultará con la empresa que incluyó los datos en el sistema para comprobar que, efectivamente, se ha procedido al pago de las cantidades pendientes.
- Encontrarse incluido en un sistema de información crediticia puede ser un verdadero quebradero de cabeza para cualquier persona que quiera tener una actividad financiera normal.

SISTEMAS DE INFORMACIÓN CREDITICIA

- Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de **CORRESPONSABLES DEL TRATAMIENTO DE LOS DATOS,** siendo de aplicación lo establecido por el **Reglamento (UE) 2016/679.**
- Corresponde al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.
- **LA PRESUNCIÓN DE LICITUD** no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo **un perfilado del mismo**, en particular mediante **la aplicación de técnicas de calificación crediticia.**

FICHERO DE
SOLVENCIA PATRIMONIAL
NOTEBOOK
NOTEBOOK 120 sheets

CONFILEGAL
INFORMACIÓN LEGAL DE CONFIANZA
ACCEDER
Miércoles 23 de Septiembre de 2015

Los FICHEROS DE SOLVENCIA PATRIMONIAL, una realidad a tener en cuenta

Dom, 20/09/2015 - 19:00

Javier Puyol, abogado y socio de Ecix Group

Share 39
Share 4
Tweet 8
googleplus 2
evernote 0
meneame 1

Los ficheros de solvencia patrimonial son aquellos creados o mantenidos por una empresa dedicada a la prestación de servicios de información patrimonial y en el que se guardan datos relativos al cumplimiento de obligaciones dinerarias por parte de personas y empresas. Tal como indica el diario Expansión, cuando una persona, física o jurídica, acude a una entidad financiera a solicitar una operación de financiación, ya se trate de un crédito, un préstamo, tarjeta de crédito o cualquier otra, se inicia por parte de la entidad un análisis de riesgo.

Dentro de éste, uno de los primeros pasos es solicitar a una empresa de prestación de servicios patrimoniales información sobre el incumplimiento por parte del solicitante de obligaciones dinerarias con otras entidades financieras u otras empresas; para ello las empresas de prestación de servicios patrimoniales cuentan con ficheros de solvencia, comúnmente llamados ficheros de "morosos".

Javier Puyol

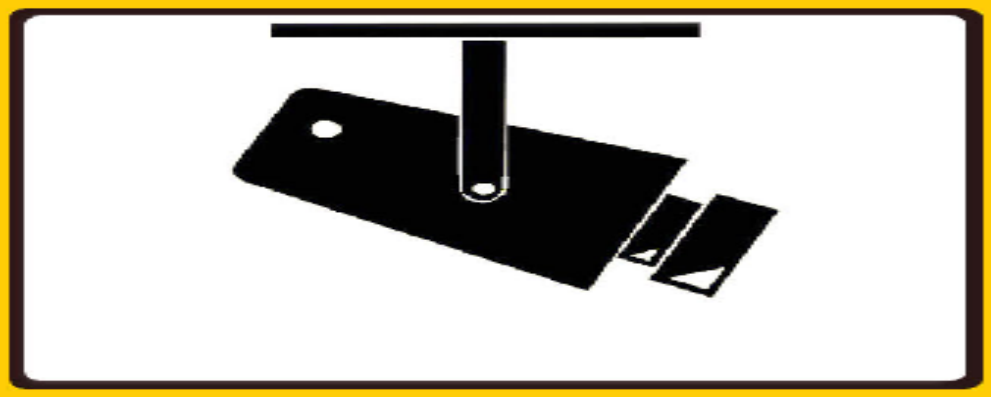
FICHEROS DE SOLVENCIA PATRIMONIAL

- Los **FICHEROS DE SOLVENCIA PATRIMONIAL** son aquellos creados o mantenidos por una empresa dedicada a la prestación de servicios de información patrimonial y en el que se guardan datos relativos al cumplimiento de obligaciones dinerarias por parte de personas y empresas.
- Cuando una persona, física o jurídica, acude a una **entidad financiera** a solicitar una operación de financiación, ya se trate de un crédito, un préstamo, tarjeta de crédito o cualquier otra, se inicia por parte de la entidad **un análisis de riesgo.**

TRATAMIENTOS RELACIONADOS CON LA REALIZACIÓN DE DETERMINADAS OPERACIONES MERCANTILES.

- Salvo prueba en contrario, **se presumen lícitos los TRATAMIENTOS DE DATOS, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier OPERACIÓN DE MODIFICACIÓN ESTRUCTURAL DE SOCIEDADES O LA APORTACIÓN O TRANSMISIÓN DE NEGOCIO O DE RAMA DE ACTIVIDAD EMPRESARIAL**, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.
- En el caso de que la operación no llegara a concluirse, la entidad cesionaria debe proceder con carácter inmediato a **la supresión de los datos**, sin que sea de aplicación la obligación de bloqueo prevista en **la ley orgánica.**

ZONA VIDEOVIGILADA



RESPONSABLE:

PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:

MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:

CARTEL ZONA VIDEOVIGILANCIA RGPD HOMOLOGADO EN 2019

- El **CARTEL DE ZONA VIDEOVIGILANCIA** es uno de los documentos necesarios para **cumplir la normativa de Protección de Datos**.

- **EN QUÉ CONSISTE**

- La videovigilancia debe estar regulada conforme a la ley de protección de datos, es decir, su empresa debe tener los carteles informativos de que se están utilizando cámaras de videovigilancia.

- **¿QUÉ HAY QUE PONER?**

- Para que el cartel esté homologado debe contener visiblemente el **nombre y la dirección de la empresa**.

- **¿DÓNDE LOS TENGO QUE COLOCAR?**

- Deben situarse en un **lugar visible** para que todas las personas que acceden a tu empresa sean conscientes de que se están utilizando cámaras de videovigilancia.

- **¿CUÁNTOS NECESITO INSTALAR?**

- Como mínimo necesitas colocar un cartel en **cada puerta de entrada** a la empresa.

- **¿TENGO QUE COLOCAR LOS CARTELES DENTRO DE LA EMPRESA?**

- Es obligatorio colocar carteles en el interior si dentro del local o establecimiento se realizan grabaciones de imágenes.

TRATAMIENTOS CON FINES DE VIDEOVIGILANCIA

- Las personas físicas o jurídicas, públicas o privadas, pueden llevar a cabo el **TRATAMIENTO DE IMÁGENES A TRAVÉS DE SISTEMAS DE CÁMARAS O VIDEOCÁMARAS** con la finalidad de **preservar la seguridad de las personas y bienes, así como de sus instalaciones.**
- Solo pueden captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad anterior.
- No obstante, es posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.
- Los datos deben ser suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.
- En tal caso, las imágenes deben ser puestas a disposición de la autoridad competente en **un plazo máximo de 72 horas** desde que se tuviera conocimiento de la existencia de la grabación.
- No es de aplicación a estos tratamientos la obligación de bloqueo de datos.

TRATAMIENTOS CON FINES DE VIDEOVIGILANCIA

- El **deber de información** se entiende cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en el **RPD.**
- También puede incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.
- En todo caso, el responsable del tratamiento debe mantener a disposición de los afectados la información anterior.
- Se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.
- Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

TRATAMIENTOS CON FINES DE VIDEOVIGILANCIA

- El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por **las Fuerzas y Cuerpos de Seguridad** y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.
- Fuera de estos supuestos, dicho tratamiento se rige por su legislación específica y supletoriamente por el Reglamento (UE) y la ley orgánica.
- Esta regulación se entiende sin perjuicio de lo previsto en la **Ley 5/2014, de 4 de abril, de Seguridad Privada** y sus disposiciones de desarrollo.
- El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de la ley orgánica.

Excmo. Ayuntamiento de CÁRTAMA

CÓMO EVITAR LA PUBLICIDAD NO DESEADA

OMIC

1 Inscríbete en la Lista Robinson

La Lista Robinson, gestionada por ADIGITAL, es un fichero de exclusión publicitaria. Al inscribirte en ella **puedes elegir el medio o canal a través del cual no quieres recibir publicidad**. La inscripción es eficaz a partir del tercer mes.

2 Utiliza las fórmulas que te ofrecen

Algunas empresas ofrecen sistemas para que puedas **rechazar el uso de tus datos** con fines publicitarios como **marcando una casilla, enviando un email, un SMS, pinchando un enlace o llamando a un número de teléfono.**

3 Evita dar tu consentimiento

En muchas ocasiones cuando participamos en un concurso o aprovechamos ofertas o descuentos nos solicitan el consentimiento para enviarnos publicidad. **Si no estás de acuerdo, no tengas reparos en negarte.**

4 Ejerce tus derechos

Puedes hacerlo en cualquier momento y, si no sabes a dónde dirigirte, solicita la información a quien está tratando tus datos o consulta su página web.

Derecho de oposición
Te permite solicitar que no se traten tus datos con fines publicitarios.

Anular el consentimiento
Si has autorizado recibir publicidad, puedes revocar en cualquier momento el consentimiento dado con anterioridad y oponerte a que se traten tus datos en acciones de marketing.

5 Puedes optar por la mediación

Si has reclamado ante las compañías y no estás satisfecho, **Autocontrol ofrece un sistema gratuito de mediación voluntaria**, al que se han adherido varias compañías de telecomunicaciones. Este sistema **funciona de forma independiente** a las reclamaciones que se pueden seguir realizando ante la Agencia.

6 Reclama ante la AEPD

Si después de inscribirte en la Lista Robinson o ejercer tus derechos ante el responsable sigues recibiendo publicidad no deseada **puedes presentar una reclamación por correo o en la Sede Electrónica de la AEPD.**

La documentación que necesitas en:
www.aepd.es

https://www.listarobinson.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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.
- **SERVICIO GESTIONADO POR ADIGITAL**
- **Asociación Española de Economía Digital**
- C/Entença, 218 Entlo 7ª 08029 Barcelona, info@listarobinson.es CIF: G61668505
- Estatutos depositados en el Servicio de Depósitos del Ministerio de Trabajo.

LISTAS ROBINSON

DE EXCLUSIÓN PUBLICITARIA

ACOSO TELEFÓNICO

- El acoso, hostigamiento o "stalking", como se denomina en inglés, se puede hacer mediante mensajes, llamadas o en persona.

ACOSO TELEFÓNICO

“STALKING” U HOSTIGAMIENTO

- La **Ley Orgánica 1/2015 de 30 de marzo** de REFORMA del Código Penal-, puso fin a esta situación de desprotección introduciendo en el Título VI, Capítulo III, un nuevo tipo penal contra la libertad: el denominado **delito de acoso** -“stalking” u hostigamiento-, regulado en el **artículo 172. ter del Código Penal**.
- 1.- Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que **acose** a una persona llevando a cabo de **forma insistente y reiterada**, y **sin estar legítimamente autorizado**, alguna de las conductas siguientes y, de este modo, **altere gravemente el desarrollo de su vida cotidiana**:
- 1.ª La vigile, la persiga o busque su cercanía física.
- 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.
- 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.
- 4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.
- Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.
- 2.- Cuando el ofendido fuere alguna de las **personas a las que se refiere el apartado 2 del artículo 173**, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso **no será necesaria la denuncia** a que se refiere el apartado 4 de este artículo.
- 3.- Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.
- 4.- Los hechos descritos en este artículo **sólo serán perseguibles mediante denuncia de la persona agraviada** o de su representante legal.

¿DÓNDE RECLAMO EL ACOSO TELEFÓNICO?

- Si después de ejercer tus derechos o poner en práctica las sugerencias anteriores continúas recibiendo publicidad no deseada, puedes presentar una reclamación en la **Agencia Española de Protección de Datos.**
- Si optas por presentar **una reclamación ante la Agencia** es necesario que aportes determinada información que sólo tú estás en disposición de proporcionar y sin la cual no resulta posible que la AEPD esclarezca las circunstancias en las que se realizó el envío de la publicidad no deseada.

ACOSO TELEFÓNICO

Así, debes aportar la siguiente documentación:

- Si recibes publicidad de una entidad de la que no eres ni has sido cliente y la has recibido transcurridos tres meses desde tu inscripción en la Lista Robinson, deberás aportar documentación acreditativa de la fecha en la que te inscribiste en la citada lista.
- Si en el momento de la contratación manifestaste a la entidad que no deseabas que tratara tus datos con fines publicitarios, deberás acompañar copia del contrato o de la documentación que acredite dicha negativa.
- Si ejerciste tu derecho de oposición o de supresión o retiraste tu consentimiento y sigues recibiendo publicidad después de un mes desde la recepción de tu solicitud por la entidad, debes aportar alguno de los siguientes documentos: la respuesta dada por el responsable del tratamiento a tu solicitud; o bien copia de la solicitud sellada por este; acuse de recibo o certificado del servicio postal o de mensajería que hayas utilizado, o cualquier otro documento o soporte que deje constancia de la recepción de tu solicitud por el destinatario. También debes acompañar esta documentación si solicitaste que se retiraran tus datos de las guías telefónicas y continuas figurando en las electrónicas al menos un mes después de la recepción de tu solicitud por el operador, o en la siguiente edición en caso de las guías editadas en forma de libro.
- Cuando se trate de publicidad enviada por medios electrónicos y la fórmula ofrecida para oponerte hubiera consistido en el envío de un SMS o en la realización de una llamada telefónica, deberás incluir imágenes del terminal móvil en las que se muestre el mensaje de solicitud de baja enviado al remitente o la llamada realizada y la fecha y hora de su envío o realización y, en su caso, de la respuesta recibida.
- Si el procedimiento ofrecido para oponerte hubiera consistido en el envío de un mensaje electrónico, deberás incluir una copia impresa del mismo, así como copia de la documentación que acredite su recepción por el destinatario (por ejemplo, acuse de recibo o lectura), las cabeceras asociadas a ese mensaje y, en su caso, la copia de la respuesta facilitada por el destinatario de la petición (si esta respuesta se remite a través de correo electrónico, debes aportar, igualmente, las cabeceras).

¿DÓNDE RECLAMO EL ACOSO TELEFÓNICO?

Finalmente es necesario que aportes la publicidad recibida, teniendo en cuenta lo siguiente:

- ❑ Si se trata de publicidad postal debes incluir una copia del envío publicitario recibido que incluya la fecha en la que se ha remitido y, si no puede deducirse de su contenido, la información que permita conocer dicha fecha, la cual puede figurar en el sobre postal correspondiente.
- ❑Si se trata de publicidad telefónica, deberás indicar, para cada llamada, el número de la línea receptora de la llamada, el nombre de la compañía con la que tenías contratado el servicio telefónico de la línea en el momento de su recepción y, si eres el abonado, documentación (factura, contrato?) que acredite la titularidad de la línea. Debes identificar asimismo a la entidad promocionada, indicando claramente si eres o has sido cliente de la misma y especificando el número de la línea llamante así como la fecha y hora en que recibiste la llamada.
- ❑Si se trata de publicidad remitida a través de SMS, debes indicar el número de la línea receptora de los mensajes, el nombre de la compañía con la que tenías contratado el servicio telefónico de la línea en el momento en que recibiste los SMS y, si eres el abonado, documentación (factura, contrato?) que acredite la titularidad de la línea. También, debes acompañar imágenes del terminal móvil receptor de los mensajes, en las que se muestre, de todos los mensajes recibidos o de una muestra suficientemente representativa, el texto completo de cada mensaje y la fecha y hora de recepción y número de línea o nombre del emisor. Generalmente, esta información puede consultarse a través de la opción ver detalle del terminal.
- ❑Si se trata de publicidad remitida a través del correo electrónico, debes aportar copia impresa del contenido completo del cuerpo de todos los mensajes recibidos o, si estos son muy numerosos, de una muestra suficientemente representativa, acompañando obligatoriamente sus cabeceras.

IDEAS QUE AYUDAN
www.ideasqueayudan.com
How can I help you?
listening...
APLICACIONES PARA GRABAR
LLAMADAS TELEFÓNICAS

¿DÓNDE RECLAMO EL ACOSO TELEFÓNICO?

- En los supuestos de acoso telefónico puedes acudir a los Órganos de Consumo de las distintas Administraciones Públicas y presentar una reclamación en materia de consumo. Conviene tener presente que realizar propuestas no deseadas y reiteradas por teléfono, fax, correo electrónico u otros medios de comunicación a distancia constituye una infracción en materia de consumo, salvo en las circunstancias y en la medida en que esté justificado legalmente para hacer cumplir una obligación contractual.
- Este tipo de prácticas se consideran agresivas por acoso y son desleales con los consumidores.

¿Cómo realizar LLAMADAS COMERCIALES cumpliendo el RGPD?

Informar en la recogida de datos

Facilitar el derecho de supresión

Consentimiento del tratamiento de datos

Gestión de suscripciones

Consultar la Lista Robinson

AyudaLeyProteccionDatos.es

SISTEMAS DE EXCLUSIÓN PUBLICITARIA

- Los **SISTEMAS DE EXCLUSIÓN PUBLICITARIA** permiten a **los responsables del tratamiento**, ya sea de manera individual o a través de sistemas o ficheros comunes, tratar datos personales mínimos que son necesarios **para identificar a quien se ha opuesto a recibir publicidad y a evitar su envío en este caso.**

LISTAS ROBINSON

DE EXCLUSIÓN PUBLICITARIA

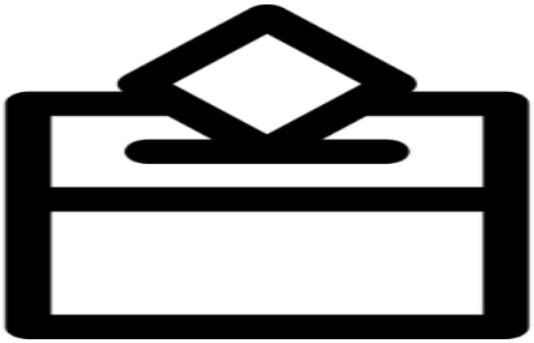
SISTEMAS DE EXCLUSIÓN PUBLICITARIA

- Es lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.
- A tal efecto, pueden crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados.
- Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.
- Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.
- La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior.
- A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

SISTEMAS DE EXCLUSIÓN PUBLICITARIA

- Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este debe informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.
- Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo.
- A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.
- No será necesario realizar la consulta anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en la ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

- **RECOPILACION Y TRATAMIENTO DE DATOS POR PARTE DE ORGANIZACIONES POLÍTICAS CON FINES DE COMUNICACIÓN POLÍTICA**



¿Cómo influye Big Data en las campañas electorales?

ARTÍCULO 58 BIS LOREG. UTILIZACIÓN DE MEDIOS TECNOLÓGICOS Y DATOS PERSONALES EN LAS ACTIVIDADES ELECTORALES.

- La **RECOPILACIÓN DE DATOS PERSONALES RELATIVOS A LAS OPINIONES POLÍTICAS DE LAS PERSONAS** que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encuentra amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.
- Los **PARTIDOS POLÍTICOS, COALICIONES Y AGRUPACIONES ELECTORALES** pueden utilizar datos personales obtenidos en páginas web y otras **fuentes de acceso público** para la realización de actividades políticas durante el periodo electoral.
- El **envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales** o medios equivalentes no tendrán la consideración de **actividad o comunicación comercial.**
- Las **actividades divulgativas** anteriores identificarán de modo destacado **su naturaleza electoral.**
- Se facilitará al destinatario de un modo sencillo y gratuito **el ejercicio del derecho de oposición.**

LISTA VIERNES

- **Propaganda electoral NO, gracias.**
- La **LISTA VIERNES** es la respuesta a una realidad alarmante: **el último cambio de la ley electoral permite a los partidos políticos utilizar tus datos de formas nuevas y preocupantes. Y queremos evitarlo.**
- Por eso, apúntate y deja clara tu postura. ¡**Es GRATIS!**
- **YO NO QUIERO PROPAGANDA**

LISTA VIERNES

- Llega la Lista Robinson de la política: Lista Viernes pretende frenar el SPAM de los partidos políticos
- **UNA MEDIDA DE PRESIÓN PARA INTENTAR ACABAR CON EL SPAM ELECTORAL**
- Por este motivo, un grupo de juristas expertos en privacidad (**Secuoya Group**) han lanzado la 'Lista Viernes': una "respuesta a una realidad alarmante" que **sirve para manifestar tu oposición al envío de propaganda electoral** a tu correo electrónico o número de teléfono.
- **El nombre de esta iniciativa se inspira** en la Lista Robinson, un servicio que sirve para evitar publicidad de empresas de las que no seas cliente o a las que no hayas facilitado tu consentimiento.
- Hay que dejar claro que al inscribirnos en la Lista Viernes **no significa que los partidos políticos vayan a dejar de enviarnos SPAM inmediatamente**. El objetivo de esta propuesta es que muchos ciudadanos se apunten y sirva como una medida de presión para que los partidos "depuren" sus bases de datos.

LISTA VIERNES

- **Afirman tener "planes mucho más ambiciosos"**
- De todos modos, los creadores de la Lista Viernes aseguran que "tienen planes mucho más ambiciosos" y creen que "**sería muy irresponsable por parte de cualquier partido político ignorar a un conjunto relevante de ciudadanos** que haya decidido oponerse activamente a la recepción de propaganda electoral por medios electrónicos".
- Los creadores de este proyecto afirman que **los datos que incluyamos en el formulario** "no serán cedidos a nadie más que a las autoridades públicas" y si no se consigue el objetivo del crowdfunding (37.300 euros) o no se alcanza "un número significativo de inscritos" se acordará la extinción de la Fundación.
- De todos modos, existen una serie de pasos que ya podemos llevar a cabo **si queremos solicitar que los partidos políticos no nos envíen propaganda** electoral por correo postal o mediante Internet.

CÓMO SOLICITAR QUE NO SE TE ENVÍE PROPAGANDA ELECTORAL POR CORREO POSTAL O POR INTERNET

XATAKA BASICS

Lo primero que tienes que hacer es entrar a la web del formulario de exclusión en las copias de censo electoral que se entregan a los representantes de las candidaturas políticas. Una vez en ella, **accede verificando tu identidad** mediante el certificado digital o la Cl@ve. Si eliges la opción Cl@ve podrás iniciar sesión con ella o solicitar el correo con el que configurarla, mientras que el certificado digital lo obtienes desde la web de la Real Casa de la Moneda.

Instituto Nacional de Estadística

@dministración electrónica

Sede Electrónica - Instituto Nacional de Estadística

Buscar

A A A

Inicio | Trámites | Normativa | Utilidades | Ayuda

07/03/2019 09:15

Está usted en Sede Electrónica / Trámites

FORMULARIO WEB DE SOLICITUD DE EXCLUSIÓN/INCLUSIÓN EN LAS COPIAS DEL CENSO ELECTORAL QUE SE ENTREGAN A LOS REPRESENTANTES DE LAS CANDIDATURAS PARA REALIZAR ENVÍOS POSTALES DE PROPAGANDA ELECTORAL

Este procedimiento permite la cumplimentación vía web de la solicitud de exclusión/inclusión en las copias del censo electoral que se entregan a los representantes de las candidaturas para realizar envíos postales de propaganda electoral.

¿Quién puede cumplimentar este formulario web de solicitud?

Cualquier persona inscrita en el censo electoral

Para realizar la solicitud se exige un certificado electrónico, reconocido por la plataforma de validación @firma del Ministerio de Política territorial y Administraciones Públicas y validado por la Oficina del Censo Electoral, o mediante el sistema Cl@ve.

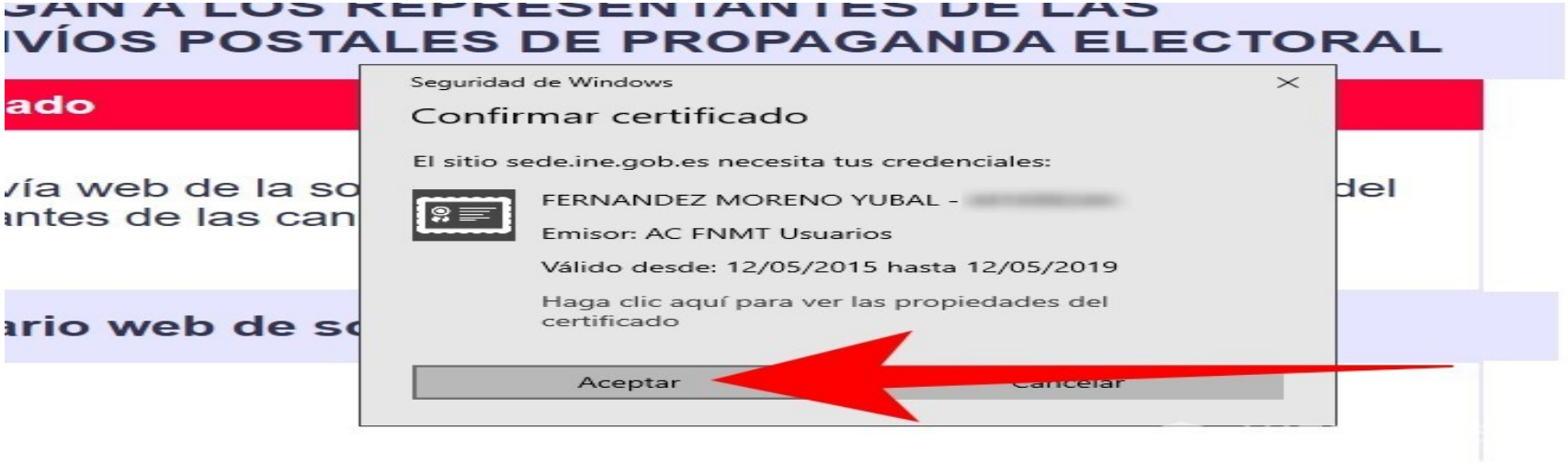
Instrucciones para la cumplimentación y envío de la solicitud

Siga las instrucciones contenidas en cada pantalla

Acceder

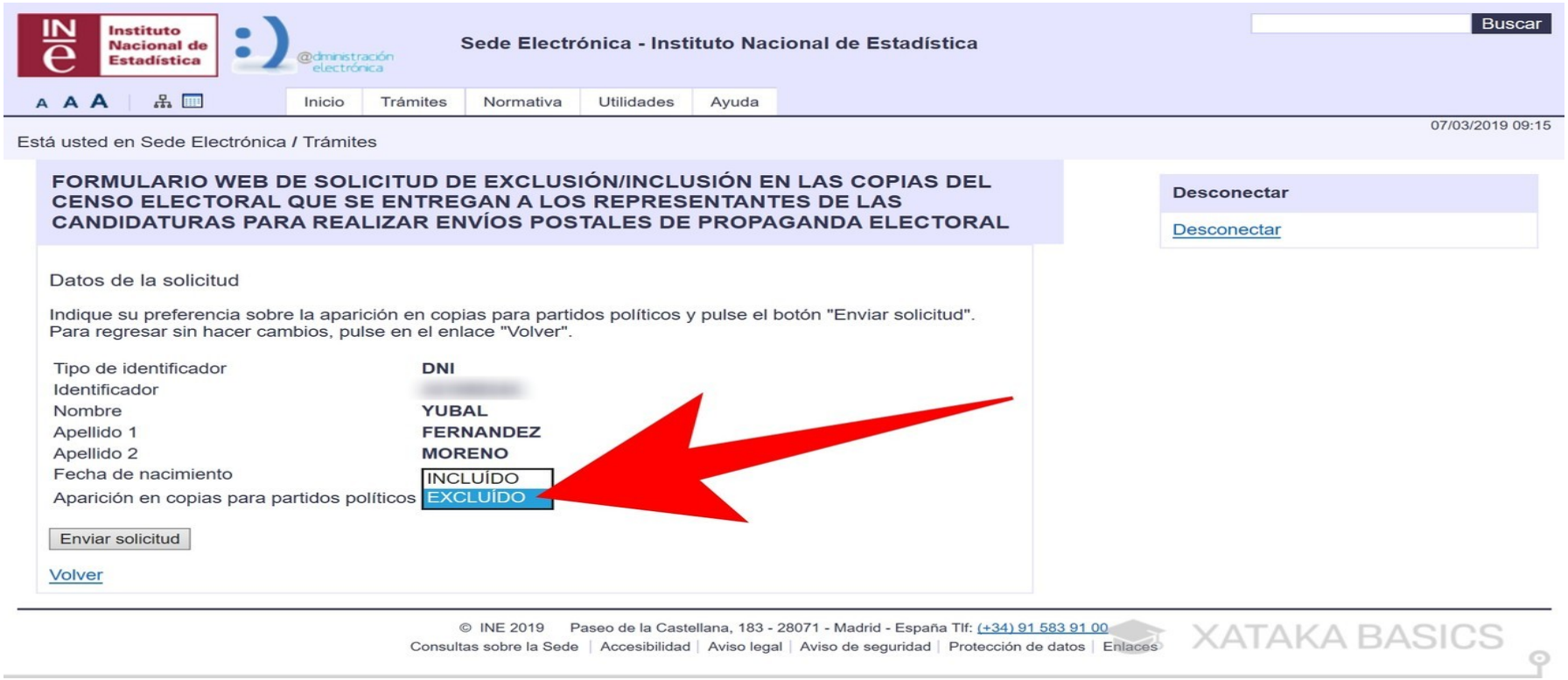
Acceder con certificado digital
Acceder con Cl@ve

En nuestro caso, hemos optado por **EL CERTIFICADO DIGITAL**, el cuál obtienes en un archivo *.pfx* que puedes instalar en Windows. **Lo más cómodo es hacer el proceso desde Microsoft Edge**, ya que no tendrás que instalar manualmente en este navegador el certificado, y recibirás una solicitud automática para utilizarlo desde el propio Windows. En cuanto a **la Cl@ve PIN**, primero tienes que registrarte con un código que recibirás por carta solicitándolo en esta web de la Agencia Tributaria, aunque también puedes registrarte con tu certificado electrónico o DNI electrónico, e incluso de forma presencial en cualquier Oficina de Registro cercana a tu casa.

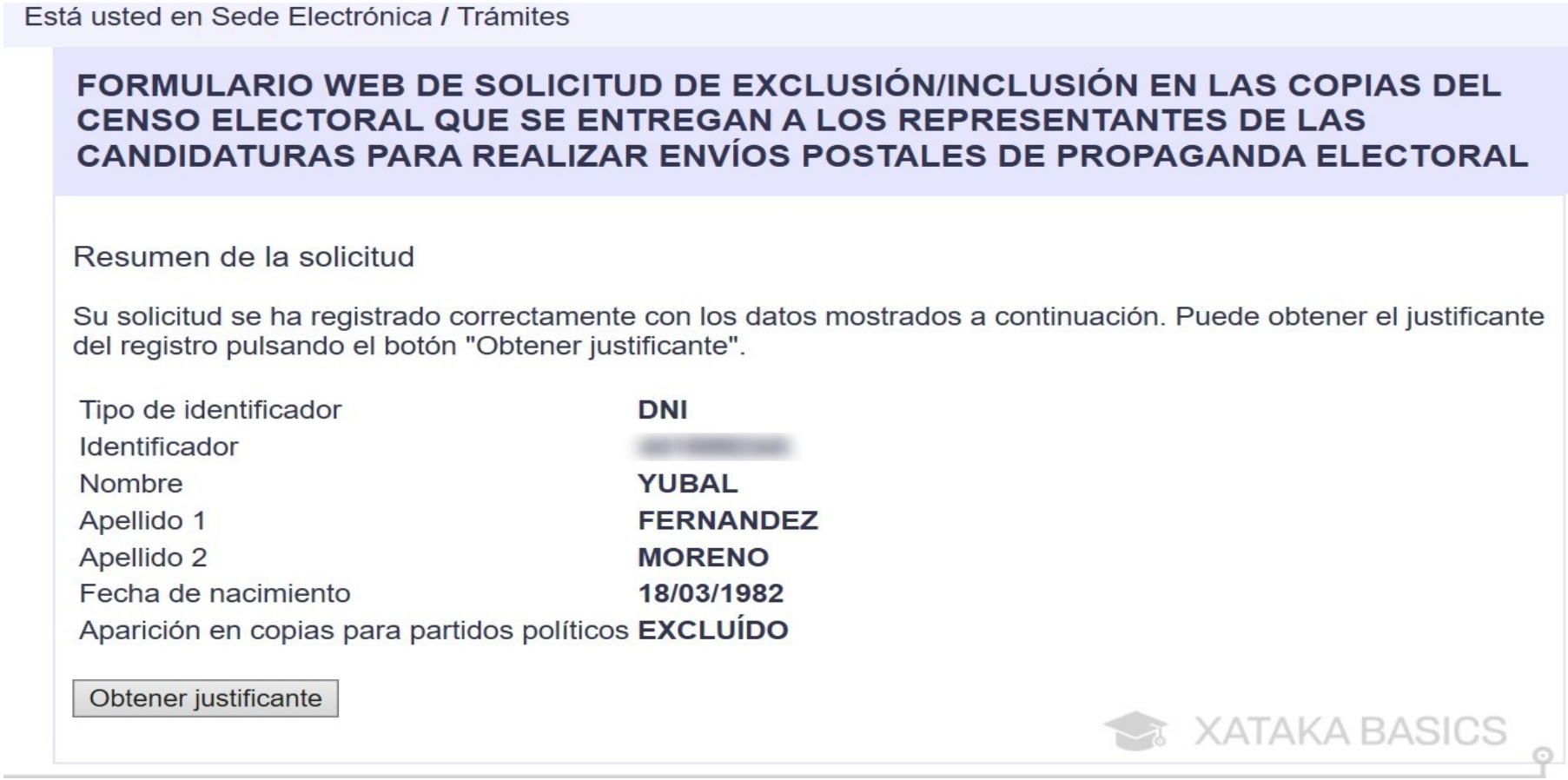


Una vez identificado, entrarás en una página en la que se te informará de tus datos, y verás que por defecto estás incluido en las copias para partidos políticos. Para cambiar esto, **pulsa en el enlace *Para solicitar la inclusión/exclusión en las copias para partidos pulse aquí*** que verás justo debajo del todo.

Al pulsar el enlace, verás que en el campo *Aparición en copias para partidos políticos* ahora hay un cuadro que si pulsas sobre él te da dos opciones. Abre el cuadro, **elige la opción *EXCLUIDO* y pulsa en el botón *Enviar solicitud*** para pedirle al Instituto Nacional de Estadística que no comparta tus datos con los partidos, de manera que estos no te puedan enviar por correo postal su propaganda.



Y ya está. Cuando pulses en *Enviar solicitud* se confirmará tu petición, y verás cómo **ahora apareces como excluído** el envío de copias para partidos políticos. Una vez se ha confirmado el trámite, podrás obtener un justificante para imprimirlo y tenerlo en estado físico.



Aparición en copias para partidos políticos

EXCLUÍDO

Estimación

Examinada su solicitud de exclusión de las copias del censo electoral que se entregan a los representantes de las candidaturas para realizar envíos postales de propaganda electoral, se le comunica que la misma ha sido estimada y tendrá efecto permanente mientras no se manifieste en sentido contrario.

Si imprimes el justificante, verás que abajo del todo pone que ***"tendrá efecto permanente mientras no se manifieste en sentido contrario"***, lo que quiere decir que ya no tendrás que volver a repetir este trámite hasta que no quieras volver a cambiar tu estado.

CÓMO SOLICITAR QUE NO TE ENVÍEN SPAM CON PROPAGANDA ELECTORAL

CÓMO SOLICITAR QUE NO TE ENVÍEN SPAM CON PROPAGANDA ELECTORAL

- ¿Y qué pasa con el famoso "spam electoral" y el envío de publicidad en formato digital que se aprobó a finales del 2018 con la nueva Ley de Protección de Datos?
- es posible solicitar que no te lo envíen, aunque con un método algo más complicado.
- Lo que tendrías que hacer, dado que al final lo que se produce es un tratamiento de datos, es **ejercer el derecho de oposición para que no te enviaran propaganda digital**. Esto evitaría que te manden deliberadamente a tí determinada publicidad, aunque seguirías estando sometido a las publicaciones patrocinadas genéricas que los partidos paguen en las redes sociales. Pero evitarías una mayor personalización de la publicidad, y que te llegue, por ejemplo, a tu correo electrónico.

SOLICITO

La oposición al tratamiento de mis datos personales, teniendo en consideración que:

☐ El tratamiento de mis datos personales se basa en una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, debiendo limitarse el tratamiento de los mismos hasta que obtenga respuesta del ejercicio de este derecho.

☐ El tratamiento de mis datos personales se basa en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, debiendo limitarse el tratamiento de los mismos hasta que se obtenga respuesta del ejercicio de este derecho.

☐ El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

Sin perjuicio de que corresponde al responsable del tratamiento acreditar motivos legítimos imperiosos que prevalezcan sobre mis intereses, derechos y libertades (en los dos primeros supuestos), o una misión realizada en interés público (en el tercer supuesto), acredito como situación personal para oponerme al tratamiento de mis datos personales

XATAKA BASICS

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

CÓMO SOLICITAR QUE NO TE ENVÍEN SPAM CON PROPAGANDA ELECTORAL

- Para ejercer tu derecho de oposición, tienes que escribir a los partidos políticos solicitando que se borren los datos que corresponda, y oponiéndote a que sean tratados en un futuro para ello. **Existen algunos documentos estándar creados para que sólo tengas que rellenar tus datos** sin preocuparte de la redacción, como por ejemplo el que puedes encontrar en la web de la Agencia Española de Protección de Datos. Esta sería la parte sencilla del proceso.
- La parte complicada es que ahora tendrás que **buscar por tu cuenta las direcciones de los delegados de protección de datos de cada partido** y enviarle a cada uno de ellos la carta una vez la hayas rellenado. La buena noticia es que se puede hacer por correo electrónico, y el de estos delegados suele aparecer en sus páginas sobre política de privacidad, como es el caso de PSOE, PP, Podemos , Ciudadanos o Vox.

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

- Los **SISTEMAS DE DENUNCIAS INTERNAS en las organizaciones** tienen **por OBJETO** que, a través de los mismos, pueda ponerse en conocimiento de una entidad privada, incluso **de manera anónima**, la comisión dentro de la misma o por terceros que contraten con aquélla, **de actos o conducta que puedan ser contrarios a la normativa, general o sectorial, aplicable.**

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

- Es lícita la creación y mantenimiento de **sistemas de información** a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.
- **Los empleados y terceros** deben ser informados acerca de la existencia de estos sistemas de información.

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

- El acceso a los datos contenidos en estos sistemas queda limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, **desarrollen las funciones de control interno y de cumplimiento**, o **a los encargados del tratamiento que eventualmente se designen a tal efecto.**
- No obstante, es lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.
- Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permite al personal con funciones de gestión y control de recursos humanos.

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

- Deben adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.
- Los datos de quien formule la comunicación y de los empleados y terceros deben conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

- En todo caso, transcurridos 3 meses desde la introducción de los datos, debe procederse a **su supresión del sistema de denuncias,** salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica.
- Las denuncias a las que no se haya dado curso solamente pueden constar **de forma ANONIMIZADA**, sin que sea de aplicación la obligación de bloqueo prevista en la ley orgánica.
- Transcurrido el plazo anterior, los datos pueden seguir siendo tratados, por el órgano al que corresponda, en la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.
- Los principios anteriores son aplicables a los **SISTEMAS DE DENUNCIAS INTERNAS** que pudieran crearse en las Administraciones Públicas.

TRATAMIENTO DE DATOS EN EL ÁMBITO DE LA FUNCIÓN ESTADÍSTICA PÚBLICA

Instituto de Estadística y Cartografía de Andalucía
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

La organización estadística en España

http://www.ine.es/ss/Satellite?L=es_ES&c=Page&cid=1254735904936&p=1254735904936&pagename=INE%2FINELayout

La **Ley 12/1989**, de 9 de mayo, **de la Función Estadística Pública** es la norma legal básica para el ejercicio de la actividad estadística en la Administración General del Estado (AGE).

En ella se establece que **la función estadística se desarrolla** por: el **Instituto Nacional de Estadística**, las **unidades de los departamentos ministeriales** y de cualesquiera otras entidades públicas dependientes de la AGE a las que se les haya encomendado aquella función y el **Consejo Superior de Estadística**, a los que se debe añadir la **Comisión Interministerial de Estadística** y el **Comité Interterritorial de Estadística**.

- **Real Decreto 1572/1993**, de 10 de septiembre, por el que se aprueba el **REGLAMENTO DE PROCEDIMIENTO ADMINISTRATIVO SANCIONADOR DE LAS INFRACCIONES POR INCUMPLIMIENTO DE LAS OBLIGACIONES ESTABLECIDAS EN LA LEY DE LA FUNCIÓN ESTADÍSTICA PÚBLICA.**

INE Instituto Nacional de Estadística

Principios generales de la función estadística pública

– secreto estadístico,
– transparencia,
– especialidad,
– proporcionalidad,
– independencia,
– accesibilidad y
– compromiso de calidad

Tomados de la legislación de la U.E.

TRATAMIENTO DE DATOS EN EL ÁMBITO DE LA FUNCIÓN ESTADÍSTICA PÚBLICA

FUNCIÓN ESTADÍSTICA PÚBLICA.

- **CONCEPTO.** La recogida y tratamiento de datos de carácter personal, con fines públicos, para la realización de "estadísticas" entendidas como "la información cuantitativa y cualitativa, agregada y representativa que caracteriza un fenómeno colectivo en una población dada".
- Se define la elaboración de estadísticas como "todas las actividades relacionadas con la recogida, el almacenamiento, el tratamiento y el análisis que se requieren para la compilación de estadísticas".
- Véase el **Informe de la Agencia Española de Protección de Datos 252/2017**

TRATAMIENTO DE DATOS EN EL ÁMBITO DE LA FUNCIÓN ESTADÍSTICA PÚBLICA

- El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se somete a lo dispuesto en su legislación específica, así como en el Reglamento (UE) y en la ley orgánica.
- La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el Reglamento (UE) en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.
- De conformidad con lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.
- Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por **las garantías del secreto estadístico** previstas en la legislación estatal o autonómica.

TRATAMIENTO DE DATOS CON FINES DE ARCHIVO EN INTERÉS PÚBLICO POR PARTE DE LAS ADMINISTRACIONES PÚBLICAS.

- Es lícito el **TRATAMIENTO POR LAS ADMINISTRACIONES PÚBLICAS DE DATOS CON FINES DE ARCHIVO EN INTERÉS PÚBLICO**, que se somete a lo dispuesto en el Reglamento (UE) y en la ley orgánica con las especialidades que se derivan de lo previsto en la **Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español**, en el **Real Decreto 1708/2011, de 18 de noviembre**, por el que se establece el **SISTEMA ESPAÑOL DE ARCHIVOS** y se regula el **Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos** y su régimen de acceso, así como **la legislación autonómica** que resulte de aplicación.

Infracciones y sanciones

Ley N° 30225 y su Reglamento de Contrataciones del Estado

Subdirección de Desarrollo de Capacidades
Dirección Técnico Normativa
Organismo Supervisor de las Contrataciones del Estado - OSCE

TRATAMIENTO DE DATOS RELATIVOS A INFRACCIONES Y SANCIONES ADMINISTRATIVAS

- El **tratamiento de datos relativos a infracciones y sanciones administrativas**, incluido el **mantenimiento de registros relacionados** con las mismas, exige:

❑ Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

❑ Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

TRATAMIENTO DE DATOS RELATIVOS A INFRACCIONES Y SANCIONES ADMINISTRATIVAS

- Cuando no se cumpla alguna de las condiciones anteriores, **los tratamientos de datos referidos a infracciones y sanciones administrativas** han de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.
- Fuera de los supuestos anteriores, los **tratamientos de datos referidos a infracciones y sanciones administrativas** solo son posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TRATAMIENTO DE DATOS

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO. MEDIDAS DE RESPONSABILIDAD ACTIVA

- El **RESPONSABLE DEL TRATAMIENTO** es la persona física o jurídica o autoridad pública, que decide sobre el tratamiento de los datos personales, determinando los fines y los medios de dicho tratamiento.
- En virtud del **PRINCIPIO DE RESPONSABILIDAD PROACTIVA** el **RESPONSABLE DEL TRATAMIENTO** tiene que aplicar medidas técnicas y organizativas para, en atención al riesgo que implica el tratamiento de los datos personales, cumplir y ser capaz de demostrar el cumplimiento.

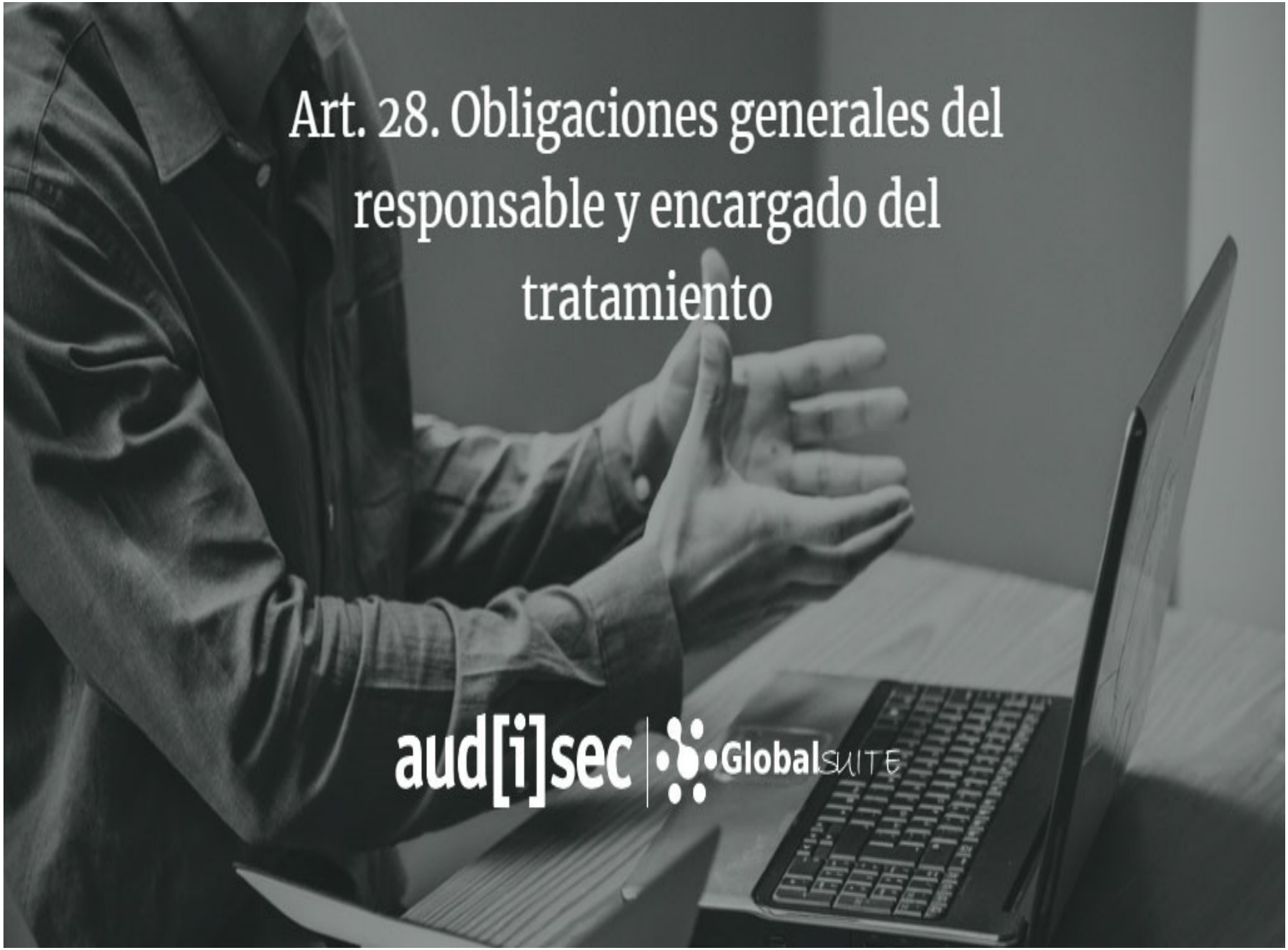
Responsable del tratamiento
Encargados
Subcontratados
Corresponsables
Destinatarios

OBLIGACIONES GENERALES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

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.


Art. 28. Obligaciones generales del responsable y encargado del tratamiento
aud[i]sec
GlobalSUITE

OBLIGACIONES GENERALES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

- El RGPD establece en los **artículos 24 y 25** que el **RESPONSABLE DEL TRATAMIENTO** debe establecer medidas para la protección de los datos desde el diseño y por defecto, es decir, aplicar a los tratamientos de datos personales las medidas técnicas y organizativas que garanticen que no son accesible a terceras personas sin la aprobación o intervención del interesado de los datos.

OBLIGACIONES GENERALES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

Partiendo de esta base, la nueva LOPD detalla que, a la hora de aplicar medidas, el **RESPONSABLE DEL TRATAMIENTO** debe tener en cuenta **el mayor riesgo que se pueda producir en los siguientes supuestos**:

- Perjuicio económico, moral o social significativo para a los interesados del tratamiento.
- Privación de derechos o control de los datos de los interesados.
- Tratamiento no incidental de categorías especiales de datos.
- Tratamiento que revele una evaluación de aspectos personales de los interesados.
- Tratamiento de datos de personas vulnerables en especial, menores o personas discapacitadas.
- Tratamiento masivo de datos, tanto en la recogida como en su tratamiento.
- Cuando se efectúen transferencias de datos a países cuyo nivel de seguridad no sea adecuado.

DATO

SUPUESTOS DE CORRESPONSABILIDAD EN EL TRATAMIENTO

- El **Reglamento Europeo (RGPD)** regula un supuesto de hecho que ha necesitado respuesta legislativa. Así, es el caso de **los TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL REALIZADOS, DE MANERA CONJUNTA, POR DOS O MÁS ENTIDADES, COMO ES EL CASO DE LOS GRUPOS EMPRESARIALES**.
- En la práctica, pueden disponer de una base de datos nutrida por las diferentes sociedades mercantiles del grupo, siendo todas éstas las que, sin distinción, deciden sobre el contenido, uso y finalidad del tratamiento de los datos

DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

apdcat

CORRESPONSABILIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

- Cada una de estas empresas del grupo ostenta la condición de **RESPONSABLE DE TRATAMIENTO**, *"Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente"*.
- Cuando estas empresas del grupo determinen conjuntamente los objetivos y los medios del tratamiento, serán considerados **CORRESPONSABLES**.
- Y, en tal caso, deben determinar, de modo transparente y de mutuo acuerdo, sus responsabilidades respectivas en el cumplimiento de las obligaciones en protección de datos; en especial, el deber de información y las relativas a la atención de los derechos de los interesados, a cuyos efectos puede fijarse a un punto de contacto en común.

CORRESPONSABILIDAD

- El grupo empresarial ha de reflejar, debidamente, en el acuerdo las **funciones** que asumen **cada uno** y dará a conocer a los interesados los aspectos esenciales del mismo.
- No obstante, los interesados, independientemente de los términos del acuerdo, pueden ejercer los derechos en protección de datos frente a, y en contra de, cada uno de los Responsables.
- El Reglamento establece que si **los responsables** participan en el mismo tratamiento, cada responsable **debe ser considerado responsable de la totalidad de los daños y perjuicios.**
- No obstante, si se acumulan en la misma causa, de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable por los daños y perjuicios causados por el tratamiento, siempre que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios.
- Todo responsable que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables que hayan participado en el mismo tratamiento.
- Con esto, los términos en los que se articule el acuerdo por parte del grupo son absolutamente relevantes, a los efectos de delimitar las responsabilidades de cada uno y no verse así en un conflicto desagradable.

REPRESENTANTES DE LOS RESPONSABLES O ENCARGADOS DEL TRATAMIENTO NO ESTABLECIDOS EN LA UNIÓN EUROPEA

ALCANCE

- La obligación de la designación de un representante surge para aquellos **responsables o encargados de tratamiento no establecidos en la UE** pero que realicen tratamiento de datos personales de interesados que residan en la UE y cuyas actividades de tratamiento estén relacionadas con ofertas de bienes o servicios a dichos interesados, o en el control de su comportamiento, es decir para toda empresa extranjera que ofrezcan bienes o servicios a residentes Europeos, o simplemente estudie el control de su comportamiento en la Unión Europea.

No es necesaria dicha designación:

- A las autoridades y organismos públicos.
- Al tratamiento ocasional siempre y cuando el mismo no suponga:
  - Un tratamiento a gran escala de datos personales de categoría especial o de condenas e infracciones penales.
  - Que sea improbable que el tratamiento entrañe riesgo para los derechos y libertades de las personas físicas.

REPRESENTANTES DE LOS RESPONSABLES O ENCARGADOS DEL TRATAMIENTO NO ESTABLECIDOS EN LA UNIÓN EUROPEA

CONTENIDO

- El Representante puede establecerse en cualquier de los Estados miembros en los que se encuentren los interesados y cuyos datos personales son tratados, bien para la oferta de bienes y servicios o bien para el estudio del comportamiento.
- Entre sus funciones se encargarán fundamentalmente la atención de las consultas de cualquier Autoridad de Control y así como de los interesados sobre cualquier asunto relativo al tratamiento de datos.
- **La designación debe constar por escrito**, y con independencia de las funciones que ostenta de cooperación con las autoridades de control o de consulta éstas últimas o de los interesados, se pueden ejercitar acciones contra el propio responsable o el encargado.
- Así mismo **el representante puede ser objeto de sanción o de medidas coercitivas en supuestos de incumplimiento por parte del responsable o del encargado**, siendo por tanto recomendable en los acuerdos de designación el establecimiento de fuertes cláusulas de indemnización en el supuesto de sanción por el incumplimiento del responsable o encargado.

REPRESENTANTES DE LOS RESPONSABLES O ENCARGADOS DEL TRATAMIENTO NO ESTABLECIDOS EN LA UNIÓN EUROPEA

CONCLUSIONES:

- Los corresponsables deben establecer por escrito el acuerdo en el que se identifique la responsabilidad de cada uno, debiendo facilitar copia o resumen el mismo a los interesados.
- Cualquier de los corresponsables puede responder de los daños y perjuicios causados, pudiendo con posterioridad repetir contra los mismos por la parte proporcional de responsabilidad que corresponda a cada uno.
- La **designación de Representante** es obligatoria para aquellos responsables o encargados no establecidos en la UE cuyas actividades de tratamiento estén relacionadas con ofertas de bienes o servicios a residentes europeos o estudios en el control de su comportamiento.
- **El Representante** puede ser responsable de los incumplimientos del responsable o encargado.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO EN EL RGPD

- Una de las **NOVEDADES** que la normativa establece es que **ya no es necesario inscribir los ficheros en la AEPD.**
- Sin embargo, se establece una **nueva obligación para el Responsable del fichero** y es la de **llevar un REGISTRO DE ACTIVIDADES DE TRATAMIENTO.**

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El (nuevo) registro (interno) de tratamientos

- ***El registro, tal como lo conocemos hoy, desaparece.***
- Se mantiene la necesidad de llevanza de un registro (interno) de las actividades de tratamiento
  - Por el Responsable
  - Por el Encargado
- Para las organizaciones:
  - Que empleen más de 250 personas, o bien:
  - Que el tratamiento entrañe riesgos para los interesados,
  - no sea ocasional
  - o incluya categorías especiales o relativos a condenas e infracciones penales.
- Dicho Registro interno estará a disposición de las Autoridades de Control

REGISTRO DE ACTIVIDADES DE TRATAMIENTO EN EL RGPD

En **el RGPD** se establece como **PRIMERA OBLIGACIÓN DEL EMPRESARIO LA ELABORACIÓN DE REGISTRO DE ACTIVIDADES DEL TRATAMIENTO** en el que debe indicarse:

- ❑ Datos que se recogen.
- ❑ Con que fin.
- ❑ Medidas de seguridad que se aplican.
- ❑ Nivel de seguridad que corresponde.
- ❑ Si el fichero es manual, mixto o automatizado.
- ❑ Si estos datos van a ser cedidos o transferidos fuera del Espacio Económico Europeo.

- **El objetivo** es que el ciudadano pueda conocer de la forma más exacta posible qué se está realizando con sus datos de carácter personal cuando los aporta a una administración pública o a una entidad privada. Y dónde puede ejercer sus derechos en protección de datos.

Curso

Aprende a hacer un registro de actividades de tratamiento

29 de octubre de 2018, lunes

CONTENIDO REGISTRO ACTIVIDADES TRATAMIENTO

El RGPD diferencia el contenido dependiendo de **si el Registro lo realiza el Responsable del fichero o el Encargado del tratamiento.**

REGISTRO DEL RESPONSABLE DEL FICHERO

Si ese registro se realiza por el Responsable del fichero debe contener:

- **Identificación** y datos de contacto de responsable, corresponsable, representante y delegado de protección de datos.
- **Fines** del tratamiento.
- Descripción de **categorías de interesados y datos**.
- Categorías de **destinatarios** existentes o previstos (inclusive en terceros países u organizaciones internacionales).
- **Transferencias internacionales** de datos y documentación de garantías para transferencias de datos internacionales exceptuadas sobre base de intereses legítimos imperiosos.

Cuando sea posible:

- Plazos previstos para supresión de datos.
- Descripción general de **medidas de seguridad**:
  - Seudonimización y cifrado de datos personales.
  - Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
  - Restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
  - Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

CONTENIDO REGISTRO ACTIVIDADES TRATAMIENTO

REGISTRO DEL ENCARGADO DEL TRATAMIENTO

El registro que debe llevar el encargado debe contener la siguiente información:

- Identificación y datos de contacto del encargado, de cada responsable por cuenta del cual actúe, del representante del encargado o del responsable, y del delegado de protección de datos.
- Las **categorías de los tratamientos** efectuados por cuenta del responsable.
- Transferencias internacionales de datos y documentación de garantías para transferencias de datos internacionales exceptuadas sobre base de intereses legítimos imperiosos.
- Cuando sea posible, una descripción general de medidas de seguridad.

Elaborar el registro de actividades de tratamiento

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

¿CÓMO DEBO ELABORAR EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO?

- Los responsables o los encargados del tratamiento deben mantener registros de las actividades de tratamiento que se encuentren bajo su responsabilidad.
- Ambos se encuentran obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros de modo que puedan servir para supervisar las operaciones de tratamiento.
- Estos registro deben constar siempre **por escrito** aunque también se consideran válidos en **formato electrónico.**

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

¿CÓMO DEBE ORGANIZARSE EL REGISTRO DE OPERACIONES DE TRATAMIENTO?

- Una posibilidad para organizar este registro de actividades de tratamiento es partir de los ficheros que actualmente han sido notificados por los responsables a la Agencia de Protección de Datos, detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos.
- No obstante, el Registro también podría organizarse en torno a **operaciones de tratamiento concretas** vinculadas a una finalidad básica común de todas ellas (por ejemplo, “gestión de clientes”, “gestión contable” o “gestión de recursos humanos y nóminas”) o con arreglo a otros criterios distintos.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

UNA VEZ ELABORADO ESE REGISTRO, ¿QUÉ HAGO CON ÉL?

- El Registro de actividades de tratamiento debe guardarse en la empresa y tenerlo siempre **actualizado y a disposición de la Autoridad de control** si ésta nos lo solicita.

¿QUÉ ME PUEDE OCURRIR SI NO TENGO ESE REGISTRO DE ACTIVIDADES DE TRATAMIENTO?

- Tanto el RGPD como la nueva LOPD consideran como **infracción grave** el no disponer de un Registro de actividades de tratamiento en los casos en que sea necesario.
- Y como tal, puede ser sancionada con multas de hasta millones de euros o el 4% del volumen global de facturación anual de la empresa.

BLOQUEO DE LOS DATOS

BLOQUEO DE LOS DATOS

- El responsable del tratamiento está obligado a bloquear los datos cuando proceda a su rectificación o supresión.
- **EL BLOQUEO DE LOS DATOS** consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.
- Transcurrido ese plazo debe procederse a la destrucción de los datos.
- Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
- Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.
- La **Agencia Española de Protección de Datos** y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

Encargado de tratamiento de datos en el RGPD

¿Cuáles son tus datos personales?

- Nombre
- Dirección
- Localización
- Perfiles digitales
- Información médica
- Ingresos
- Perfil cultural
- Otros

RECOPILAS DATOS PERSONALES EN TU NEGOCIO

Tienes que acatar la regla.

Gestionas datos personales para otras empresas

También tienes que cumplirla.

Encargado de tratamiento

Cláusulas contractuales

Objeto de las cláusulas contractuales

Naturaleza, objeto y finalidad del tratamiento

Condiciones del tratamiento

Derechos y obligaciones del responsable del tratamiento
+
Obligaciones del encargado

Condiciones para recurrir a otro encargado del tratamiento

Finalización de los servicios de tratamiento

ENCARGADO DEL TRATAMIENTO.

- 1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.
- 2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.
- Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.
- 3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.
- No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.
- 4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.
- 5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

Insight exclusivo AEC

Descubre las claves de la nueva figura del

Delegado de Protección de Datos

DPD / DPO

16 de noviembre de 2017

Eduard Chaveli

Socio – General Manager & Legal Services Director en Govertis

Organiza

AEC

Con la colaboración de

GOVERTIS

DELEGADO DE PROTECCIÓN DE DATOS

DELEGADO DE PROTECCIÓN DE DATOS. DESIGNACIÓN

Los **RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO** deben designar **UN DELEGADO DE PROTECCIÓN DE DATOS** en los supuestos previstos en el Reglamento (UE) y, en todo caso, cuando se trate de las siguientes entidades:

- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- e) Las entidades incluidas en la Ley de ordenación, supervisión y solvencia de entidades de crédito.
- f) Los establecimientos financieros de crédito.
- g) Las entidades aseguradoras y reaseguradoras.
- h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
- Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- ñ) Las empresas de seguridad privada.
- o) Las federaciones deportivas cuando traten datos de menores de edad.

DELEGADO
DE PROTECIÓN DE DATOS
ACREDITACIÓN
PARA EL EXAMEN DE
CERTIFICACIÓN DPO
MÁS INFORMACIÓN

DELEGADO DE PROTECCIÓN DE DATOS

- Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.
- Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.
- La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.
- En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

¿NECESITO UN DELEGADO DE
PROTECCIÓN DE DATOS?

CUALIFICACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

- El cumplimiento de los requisitos establecidos en el Reglamento (UE) para la designación del delegado de protección de datos, sea persona física o jurídica, puede demostrarse, entre otros medios, a través de **MECANISMOS VOLUNTARIOS DE CERTIFICACIÓN** que tienen particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

POSICIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS

- 1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.
- 2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.
- 3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.
- 4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

INTERVENCIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS EN CASO DE RECLAMACIÓN ANTE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

- Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.
- En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.
- Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.
- Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.
- El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CÓDIGOS DE CONDUCTA

CODIM

Código de Conducta

para el tratamiento de datos de carácter personal en la

Investigación de Mercados

CÓDIGOS DE CONDUCTA

- Los **CÓDIGOS DE CONDUCTA** tienen el objetivo de promover entre las entidades de un determinado sector el cumplimiento normativo.
- Cuando se realiza **un tratamiento de datos de forma habitual en un sector**, las empresas deben dar cumplimiento a la normativa de forma similar, por lo que establecen reglas comunes para ello.

AUTOCONTROL

Asociación para la Autorregulación de la Comunicación Comercial

CÓDIGOS DE CONDUCTA

- Los códigos de conducta constituyen una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse a sí mismas a partir de la normativa establecida
- Se pueden elaborar por las asociaciones y otros organismos representativos de categorías de responsables y encargados, para los que son vinculantes una vez adheridos a los 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, en lo que respecta a:

- el tratamiento leal y transparente
- los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos
- la recogida de datos personales
- la seudoanonimización de datos personales
- la información proporcionada al público y a los interesados
- el ejercicio de los derechos de los interesados
- la información proporcionada a los niños y la protección de éstos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño
- las medidas y procedimientos para garantizar la seguridad del tratamiento así como la protección de datos desde el diseño y por defecto
- la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados
- la transferencia de datos personales a terceros países y organizaciones internacionales, o
- los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativos al tratamiento, sin perjuicio de los derechos de los interesados
- Así mismo, deben incluir mecanismos que permitan efectuar el control obligatorio de su cumplimiento

CÓDIGOS DE CONDUCTA

INCENTIVOS DE LOS CÓDIGOS DE CONDUCTA

- En protección de datos los códigos de conducta 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.

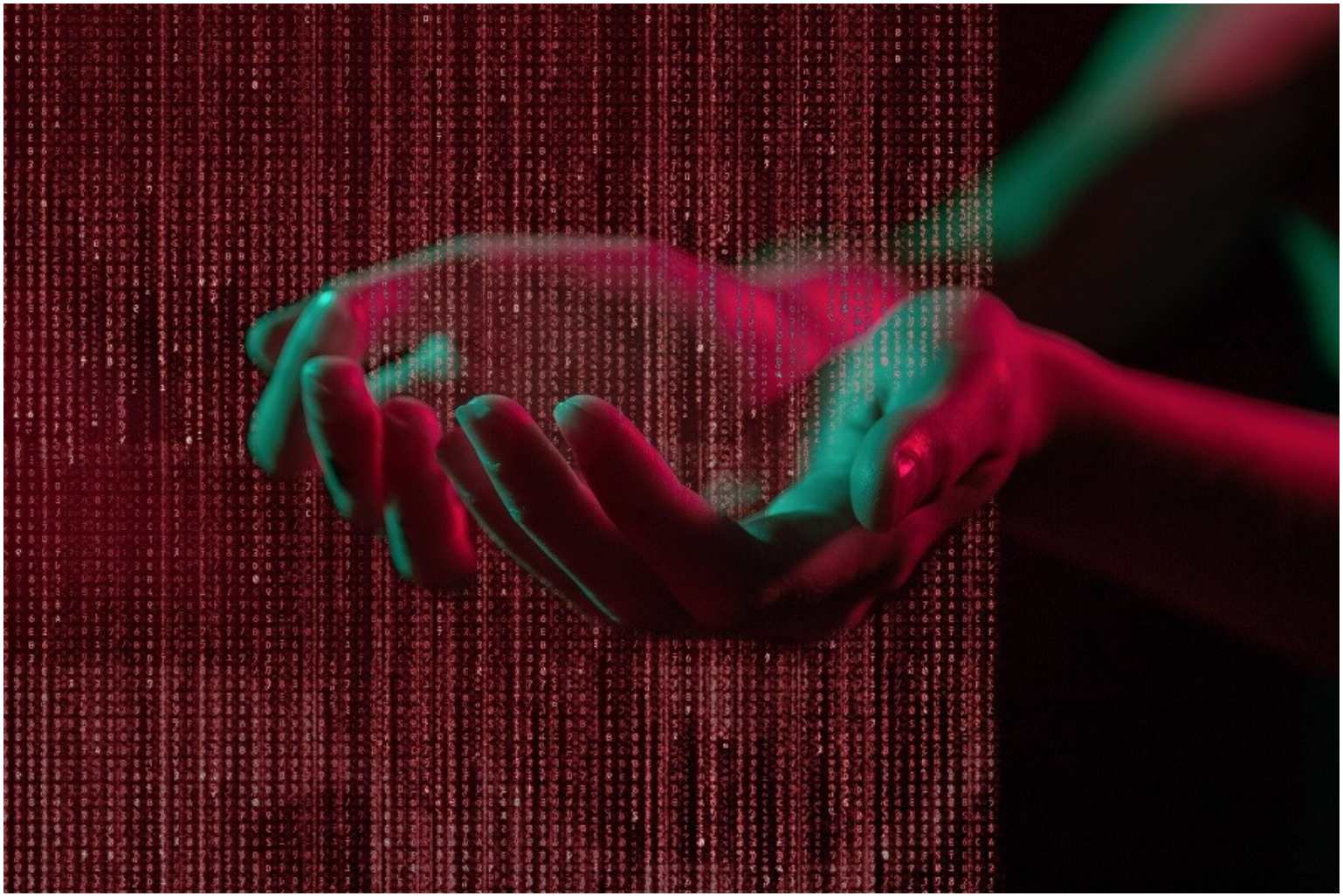
LISTADO DE LOS CÓDIGOS INSCRITOS AEPD

- CÓDIGO ÉTICO DE PUBLICIDAD Y COMERCIO ELECTRÓNICO
- CÓDIGO TIPO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DE LA ASOCIACIÓN ESPAÑOLA DE MICROPRÉSTAMOS AEMIP
- CÓDIGO DE CONDUCTA PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR ORGANIZACIONES DE INVESTIGACIÓN DE MERCADO, SOCIAL, DE LA OPINIÓN Y DEL ANÁLISIS DE DATOS
- CÓDIGO TIPO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
- CÓDIGO TIPO DEL FICHERO DE PREVENCIÓN DEL FRAUDE EN SEGUROS DE RAMOS DIVERSOS
- CÓDIGO ÉTICO DEL SECTOR DE INFORMACIÓN COMERCIAL
- CÓDIGO TIPO DE PROTECCIÓN DE DATOS PARA ORGANIZACIONES SANITARIAS PRIVADAS
- CÓDIGO TIPO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DE LA ASOCIACIÓN NACIONAL DE ENTIDADES DE GESTIÓN DE COBRO
- ANEXOS AL CÓDIGO TIPO DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL APLICABLE AL TRATAMIENTO DE DATOS DE LA OFICINA DE FARMACIA, PROMOVIDO POR EL COLEGIO DE FARMACÉUTICOS DE LA PROVINCIA DE BARCELONA
- CÓDIGO TIPO DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL APLICABLE AL TRATAMIENTO DE DATOS DE LA OFICINA DE FARMACIA, PROMOVIDO POR EL COLEGIO DE FARMACÉUTICOS DE LA PROVINCIA DE BARCELONA

LISTADO DE LOS CÓDIGOS INSCRITOS AEPD

- CÓDIGO TIPO DE PROTECCIÓN DE DATOS PERSONALES DEL FICHERO ASNEF PROTECCIÓN
- CÓDIGO TIPO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA ESTABLECIMIENTOS SANITARIOS PRIVADOS DE LA PROVINCIA DE SEVILLA
- CÓDIGO TIPO DEL FICHERO DE AUTOMÓVILES PERDIDA TOTAL, ROBO E INCENDIOS
- CÓDIGO TIPO DE FARMAINDUSTRIA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LA INVESTIGACIÓN CLÍNICA Y DE LA FARMACOVIGILANCIA
- CÓDIGO TIPO DEL SECTOR DE LA INTERMEDIACIÓN INMOBILIARIA
- CÓDIGO TIPO DE LA ASOCIACIÓN CATALANA DE RECURSOS ASISTENCIALES (ACRA)
- CÓDIGO DE CONDUCTA DE PROTECCIÓN DE DATOS PERSONALES EN LA UNIVERSIDAD DE CASTILLA-LA MANCHA
- CÓDIGO TIPO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL PARA ODONTÓLOGOS Y ESTOMATÓLOGOS DE ESPAÑA
- CÓDIGO ÉTICO DE COMERCIO ELECTRÓNICO Y PUBLICIDAD INTERACTIVA
- CÓDIGO TIPO DE LA UNIÓ CATALANA D'HOSPITALS
- CÓDIGO TIPO FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL

CERTIFICACIÓN DELEGADO DE PROTECCIÓN DE DATOS



ENTIDADES DE CERTIFICACIÓN ACREDITADAS POR ENAC

- IVAC INSTITUTO DE CERTIFICACIÓN, SL
- ASOCIACIÓN PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN, ISMS FORUM
- ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (AEC)
- ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN, ANF AC
- CUALICONTROL ACI SAU
- AENOR INTERNACIONAL, SAU
- ADOK CERTIFICACIÓN INTERNACIONAL, S.L.
- INSTITUTO DE GRADUADOS EN INGENIERÍA E INGENIEROS TÉCNICOS DE ESPAÑA (INGITE)
- BUREAU VERITAS IBERIA SL
- ITANSA CERTIFICACIONES S.L

IVAC INSTITUTO DE CERTIFICACIÓN

ITANSA CERTIFICACIONES

ANF AUTORIDAD DE CERTIFICACIÓN

¿EN QUÉ CONSISTE LA CERTIFICACIÓN?

FASE I

- Análisis candidato
- El candidato a DPD/DPO tiene que aportar los requisitos de competencia, basados en dos criterios:
  - Experiencia profesional
  - Formación

¿EN QUÉ CONSISTE LA CERTIFICACIÓN?

FASE II

- Evaluación
- Una vez validada la Fase I, se procederá a la evaluación de los conocimientos y capacidades técnicas o profesionales a través de un Examen.

¿EN QUÉ CONSISTE LA CERTIFICACIÓN?

EXAMEN

- Una vez superada la Fase I de análisis por el candidato, la evaluación de los conocimientos y capacidades técnicas o profesionales se llevará cabo mediante la realización de un examen.
- El examen tiene una duración de 4 horas y engloba un total de 150 preguntas tipo test sobre los conocimientos específicos detallados en el programa del esquema de certificación de la AEPD
- Será requisito imprescindible para la obtención del certificado la superación del examen, una vez evaluados los conocimientos teórico-prácticos del solicitante para realizar funciones de Delegado de Protección de Datos.
- Superado el examen, el candidato recibirá un certificado expedido por AENOR.

¿EN QUÉ CONSISTE LA CERTIFICACIÓN?

FASE III

- Certificación

- Renovable cada 3 años.

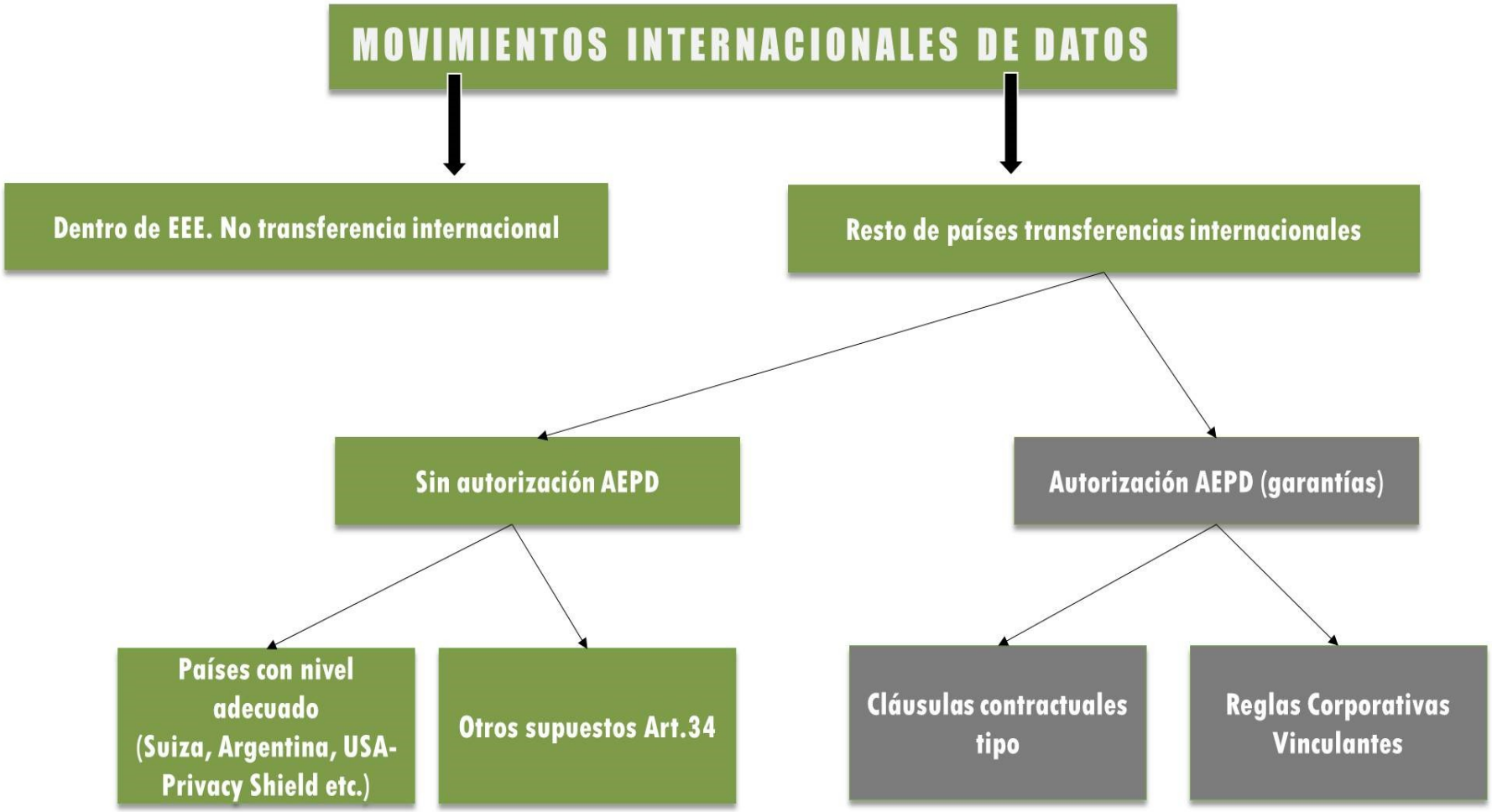
ACREDITACIÓN DE INSTITUCIONES DE CERTIFICACIÓN

- La **Agencia Española de Protección de Datos (AEPD**) ha impulsado junto con la **Entidad Nacional de Acreditación (ENAC**) el desarrollo de **UN SISTEMA DE CERTIFICACIÓN DE DPD/DPO** con el objetivo de ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones.
- Las certificaciones son otorgadas por **entidades certificadoras** debidamente acreditadas por **ENAC** como garantía de la cualificación y capacidad profesional de los **DPD/DPO.**
- Aunque la certificación no es obligatoria, proporciona gran reconocimiento y es una importante oportunidad profesional ante la futura demanda de esta figura.
- **AENOR** cuenta con la autorización provisional para **Certificar Delegados de Protección de Datos**, según lo establecido en el esquema de certificación de la **Agencia Española de Protección de Datos AEPD/DPD**, y una vez superada la revisión para la acreditación de la **Entidad Nacional de Acreditación, ENAC.**

ACREDITACIÓN DE INSTITUCIONES DE CERTIFICACIÓN

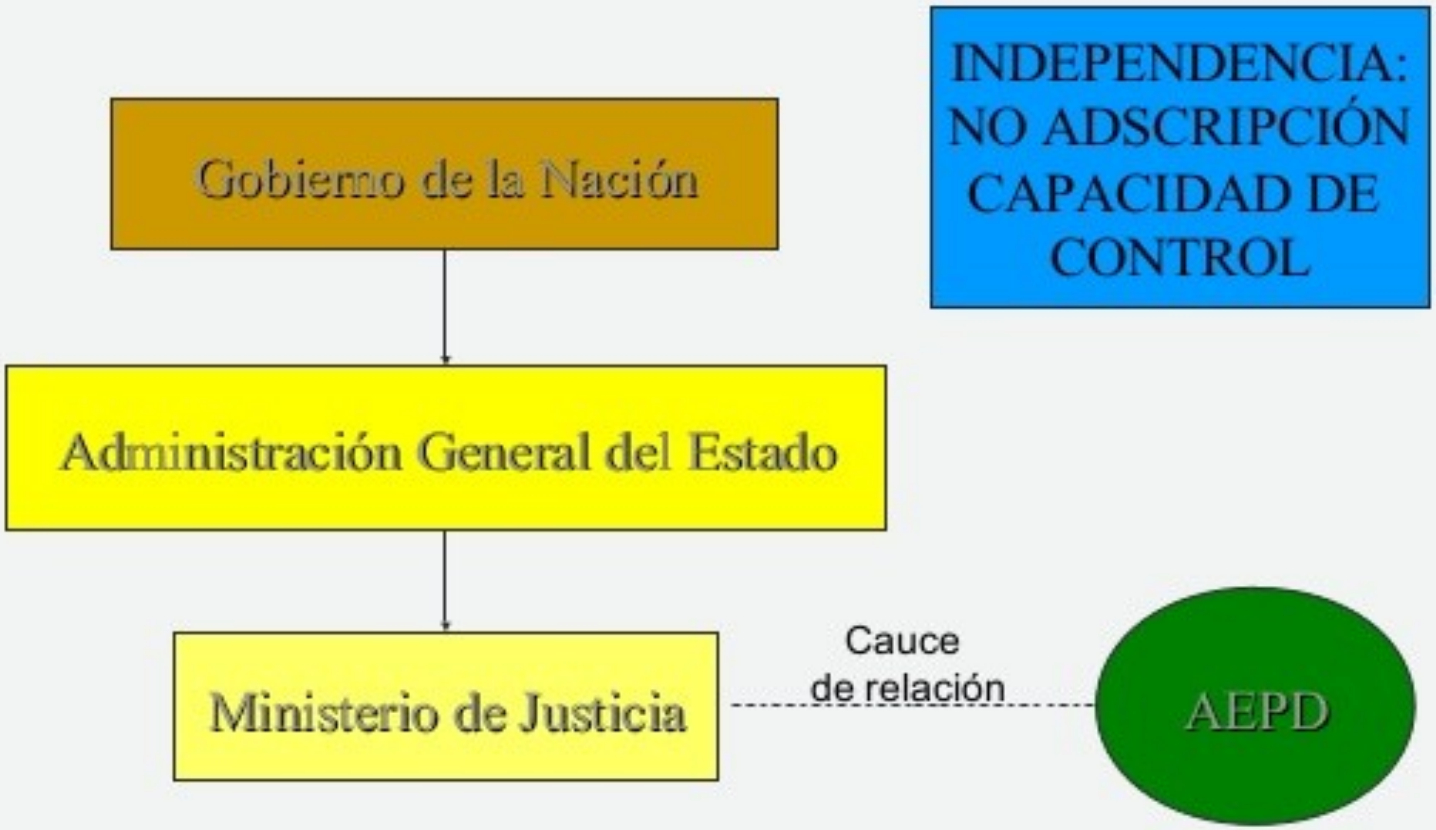
- **ENTIDADES DE CERTIFICACIÓN ACREDITADAS POR ENAC**
- Entidades de certificación acreditadas o en proceso de acreditación para expedir certificados de **DELEGADOS DE PROTECCIÓN DE DATOS** de conformidad con el **Esquema AEPD-DPD de la Agencia**:

TRANSFERENCIA INTERNACIONAL DE DATOS – PRIVACY SHIELD



AUTORIDADES DE PROTECCIÓN DE DATOS
LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

PROTECCIÓN DE DATOS EN ESPAÑA



LOS ÓRGANOS PÚBLICOS NACIONALES QUE GESTIONAN LA PROTECCIÓN DE DATOS

- La Agencia Española de Protección de Datos Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes «autoridad de control En España es esta autoridad administrativa independiente de ámbito estatal que actúa con plena independencia de los poderes públicos Su web es: www.agpd.es

AGENCIAS DE PROTECCIÓN DE DATOS AUTONÓMICAS

Las **autoridades autonómicas** actúan con las autoridades de control en sus territorios cuando se refieran a:

- Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.
- Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.
- Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

AUTORIDADES AUTONÓMICAS
DE PROTECCIÓN DE DATOS

Autoritat Catalana de Protecció de Dades

APDCM

Agencia de Protección de Datos de la Comunidad de Madrid

ESTATUTO DE AUTONOMÍA DE ARAGÓN

❑Artículo 16. **DERECHOS EN RELACIÓN CON LOS SERVICIOS PÚBLICOS.**

- 3. Todas las personas **tienen DERECHO A LA PROTECCIÓN DE SUS DATOS PERSONALES** contenidos en **las bases de datos de las Administraciones Públicas y empresas públicas aragonesas y las empresas privadas** que trabajen o colaboren con ellas. Igualmente, tienen **derecho a acceder a los mismos, a su examen y a obtener su corrección y cancelación.**

❑**COMPETENCIA COMPARTIDA**.

- Artículo 75. 5.ª **Protección de datos de carácter personal**, que, en todo caso, incluye la regulación, inscripción y el tratamiento de los mismos, el control de los ficheros creados o gestionados por las instituciones públicas de Aragón y, en especial, **la creación de una AGENCIA DE PROTECCIÓN DE DATOS DE ARAGÓN**

VENTAJAS DE UNA AGENCIA ARAGONESA DE PROTECCIÓN DE DATOS

- Mayor acercamiento y grado de concienciación por parte de los ciudadanos y los consumidores
- Mejor gestión de la ciberseguridad ampliando el control en la cadena de seguridad.
- Mayor sensibilidad por parte de los responsables de los tratamientos y encargados en el cumplimiento de sus obligaciones
- Adaptar la legislación estatal en materia de uso de medios electrónicos a las características de nuestra Comunidad
- Acceder a información directa y tener voz en la AEPD
- Atender y regular las singularidades propias de las administraciones públicas de la Comunidad de Aragón.
- Acceso sin discriminaciones a los servicios audiovisuales y a las tecnologías de la información y la comunicación (Mayor solidaridad intermunicipal –Artículo 28,2 Estatuto Autonomía)
- Fomento de la excelencia en la calidad de los servicios públicos

PROCEDIMIENTOS EN CASO DE POSIBLE VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

- El **RGPD** establece un sistema novedoso y complejo, que evoluciona hacia **un modelo de «ventanilla única»** en el que existe una autoridad de control principal y otras autoridades interesadas.
- También establece **UN PROCEDIMIENTO DE COOPERACIÓN ENTRE LAS AUTORIDADES DE LOS ESTADOS MIEMBROS** y, en caso de discrepancia, se prevé la decisión vinculante del **Comité Europeo de Protección de Datos.**
- Con carácter previo a la tramitación de cualquier procedimiento, es preciso determinar **si el tratamiento tiene o no carácter transfronterizo** y, en caso de tenerlo, **qué autoridad de protección de datos ha de considerarse principal.**

PROCEDIMIENTOS EN CASO DE POSIBLE VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

La regulación que realiza la **LOPDGDD** se limita a:

- ❑- delimitar el régimen jurídico (artículo 63);
- ❑- la iniciación de los procedimientos (artículo 64);
- ❑- la admisión o inadmisión de las reclamaciones (artículo 65);
- ❑- la determinación del alcance territorial (artículo 66)
- ❑- las actuaciones previas de investigación (artículo 67);
- ❑- el acuerdo de inicio del procedimiento (artículo 68) y
- ❑- las medidas provisionales, entre las que destaca la orden de bloqueo de los datos (artículo 69).

- Igualmente se estipulan en los citados artículos los plazos de tramitación de los procedimientos y, en su caso, su posible suspensión.
- Las especialidades del procedimiento se remiten al desarrollo reglamentario.
- Es posible que la **Agencia Española de Protección de Datos** remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta que será vinculante para quienes se adhieran al mismo.

COMIENZAN LAS SANCIONES POR LA LEY DE PROTECCIÓN DE DATOS

RÉGIMEN SANCIONADOR. SUJETOS RESPONSABLES

Están **SUJETOS AL RÉGIMEN SANCIONADOR** establecido en el **Reglamento (UE) 2016/679** y en **la LEY ORGÁNICA**:

- **Los responsables de los tratamientos.**
- **Los encargados de los tratamientos.**
- **Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.**
- **Las entidades de certificación.**
- **Las entidades acreditadas de supervisión de los códigos de conducta.**

- No es de aplicación al **DELEGADO DE PROTECCIÓN DE DATOS** el régimen sancionador establecido en este Título.

INFRACCIONES Y SANCIONES

Comparativa de incremento de sanciones del RGPD vs. LOPD

Sistel

RGPD

HASTA **10.000.000 €** O

2 % VOLUMEN DE NEGOCIO ANUAL GLOBAL DEL EJERCICIO FINANCIERO ANTERIOR

- No consentimiento menores
- No aplicar medidas técnicas y organizativas por defecto
- No dispones de registro de actividades de tratamiento
- No notificar brechas de seguridad
- No realizar la evalución de impacto
- No designar DPO

LOPD

ENTRE **900 €** Y **40.000 €** EN CASO DE INFRACCIÓN LEVE

INFRACCIONES LEVES

RGPD

HASTA **20.000.000 €** O

4 % VOLUMEN DE NEGOCIO ANUAL GLOBAL DEL EJERCICIO FINANCIERO ANTERIOR

- No cumplir con los principios del RGPD
- No cumplir con los derechos de los interesados
- No cumplir con los requisitos para transferencia internacional de datos
- No cumplir con la resolución de la Autoridad de Control

LOPD

ENTRE **40.001 €** Y **600.000 €** EN CASO DE INFRACCIÓN GRAVE O MUY GRAVE

INFRACCIONES GRAVES

En nuestra página **www.sistel.es** podrás encontrar la hoja de ruta para la aplicación del Reglamento General de Protección de Datos

La **RGPD** fue promulgada en mayo de 2016 y la fecha límite para su adopción es **25 de mayo de 2018**

SANCIONES Y MEDIDAS CORRECTIVAS

- **El RGPD** faculta a los Estados miembros a establecer normas en materia de sanciones que no sean las multas administrativas.
- La normativa española, LOPDGDD, establece que las sanciones por infracciones en materia de protección de datos), se aplicarán teniendo en cuenta los **criterios de graduación** del RGPD, **y además podrá tener en cuenta**:

❑El carácter continuado de la infracción.

❑La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

❑Los beneficios obtenidos como consecuencia de la comisión de la infracción.

❑La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

❑La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

❑La afectación a los derechos de los menores.

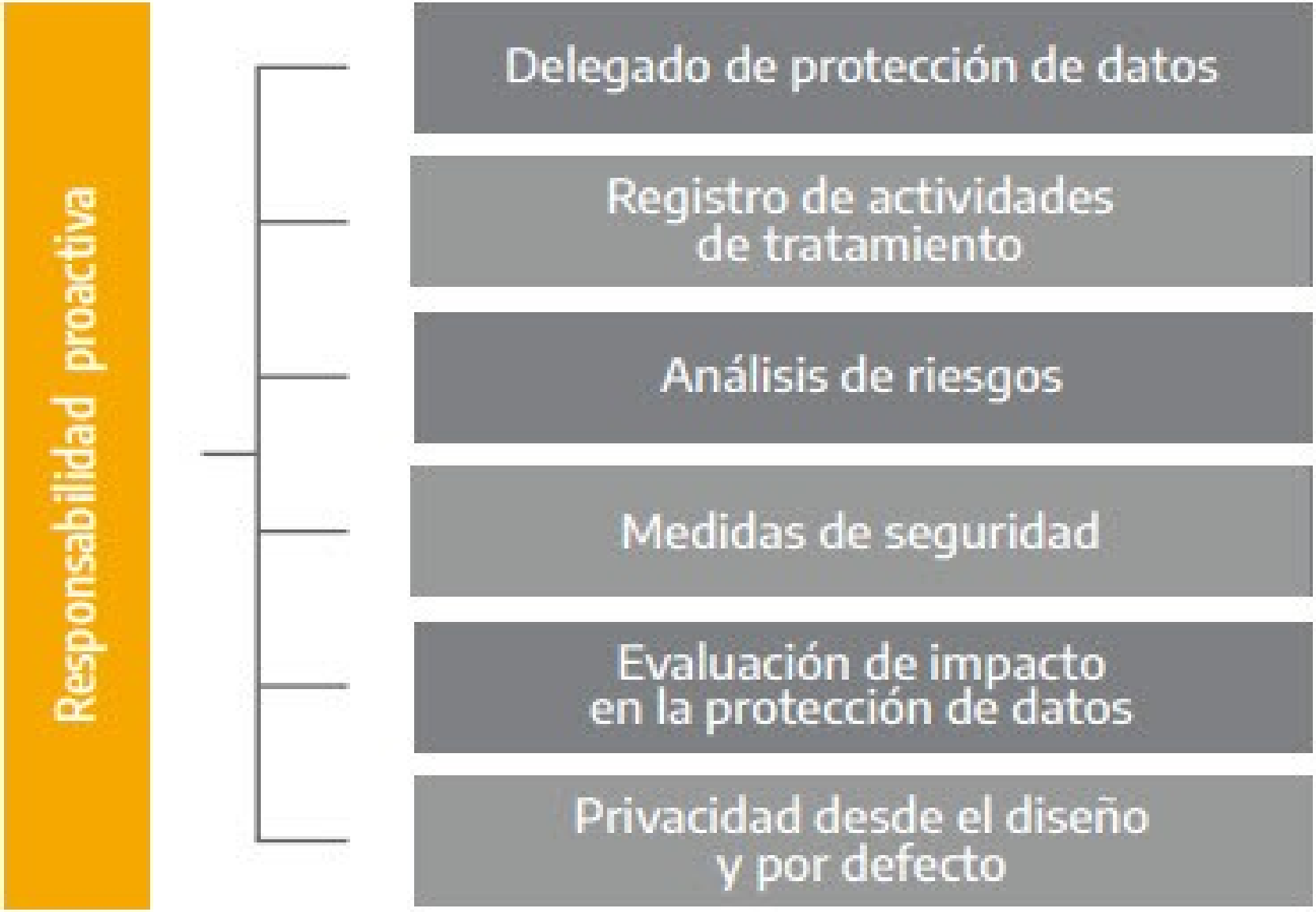
❑Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

❑El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

SANCIONES Y MEDIDAS CORRECTIVAS

- Tambien se recoge que, de modo complementario o alternativo, se podrán adoptar, cuando proceda, las **medidas correctivas** indicadas en el art. 58.2 RGPD, tales como:
- a) sancionar a todo responsable o encargado del tratamiento con una **advertencia** cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el RGPD;
- b) sancionar a todo responsable o encargado del tratamiento con **apercibimiento** cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RGPD;
- c) ordenar al responsable o encargado del tratamiento que **atiendan las solicitudes de ejercicio** de los derechos del interesado;
- d) ordenar al responsable o encargado del tratamiento que las o**peraciones de tratamiento se ajusten a las disposiciones** del RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado;
- e) ordenar al responsable del tratamiento que **comunique al interesado las violaciones de la seguridad**;
- f) imponer una **limitación temporal o definitiva** del tratamiento, **incluida su prohibición**;
- g) **ordenar la rectificación o supresión** de datos personales **o la limitación de tratamiento** y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales;
- h) **retirar una certificación, ordenar** al organismo de certificación **que retire una certificación** emitida, **o que no se emita** una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;
- j) **ordenar la suspensión de los flujos** de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.
-
- Además se establece que, cuando sea competente la AEPD, en los casos en que la sanción fuese superior a 1 millón de euros y el infractor sea una persona jurídica, se publicará el en BOE la información que identifique al infractor, la infracción cometida y el importe de la sanción. Si la competencia fuese de una autoridad autonómica (País Vasco, Cataluña o Andalucía), se estará a lo que disponga su propia normativa.
- Evidentemente, todas las sanciones, o medidas correctivas aplicadas, deberán ser efectivas, proporcionadas y disuasorias.

MEDIDAS SEGURIDAD PD


Responsabilidad proactiva
Delegado de protección de datos
Registro de actividades de tratamiento
Análisis de riesgos
Medidas de seguridad
Evaluación de impacto en la protección de datos
Privacidad desde el diseño y por defecto

Responsabilidad activa

Tipos de medidas

- Mantener "registro de actividades de tratamiento"
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación

¿Qué medidas de seguridad me exige el nuevo reglamento de protección de datos?

@lexblogger_

MEDIDAS SEGURIDAD RGPD ORGANIZATIVAS
Deber de confidencialidad y secreto

- Debe **impedirse el acceso a datos personales de personas no autorizadas**. Para ello intenta no dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.). Esto incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
- Los documentos en papel y soportes electrónicos se almacenarán en **lugar seguro** (armarios o estancias de acceso restringido) durante las 24 horas del día.
- No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
- No se comunicarán datos personales o cualquier información personal a terceros. Ni divulgarse datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

MEDIDAS SEGURIDAD RGPD ORGANIZATIVAS
DERECHOS DE LOS TITULARES DE LOS DATOS

- Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión y oposición. El responsable del tratamiento deberá responder a los interesados lo antes posible.
- En caso de ejercicio del **derecho de acceso** se facilitará a los interesados:
  - lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos,
  - identidad de los destinatarios de los datos,
  - plazos de conservación e
  - identidad del responsable ante el que solicitar la rectificación, supresión y oposición al tratamiento de los datos.
- En caso de solicitarse la **rectificación** se modificarán los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
- Cuando se solicite la **supresión**, se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

MEDIDAS SEGURIDAD RGPD ORGANIZATIVAS
VIOLACIONES DE SEGURIDAD DE DATOS

- Cuando se produzcan violaciones de seguridad de datos personales, como por ejemplo, el robo o acceso indebido a los datos personales, **se notificará a la Agencia Española de Protección de Datos** en 72 horas desde que de dichas violaciones de seguridad tuvieron lugar.
- Y debe añadirse toda la información necesaria para la aclaración de los hechos que produjeron el acceso indebido a los datos personales.
- La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

MEDIDAS SEGURIDAD RGPD TECNICAS
IDENTIFICACIÓN DE USUARIOS

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades.
- Es importante **separar los usos personales y profesionales** del ordenador.
- Una recomendación es tener perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin derechos de administración o privilegios para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de **contraseñas para el acceso** a los datos personales almacenados en sistemas electrónicos. Las contraseñas deben mezclar números y letras, teniendo al menos 8 caracteres.

MEDIDAS SEGURIDAD RGPD TECNICAS

DEBER DE SALVAGUARDA

- **ACTUALIZACIÓN DE DISPOSITIVOS Y ORDENADORES**. Los ordenadores y dispositivos usados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- **MALWARE**: Se dispondrá de un sistema de antivirus en los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales que garantice la protección de la información y datos personales. Este sistema debe actualizarse periódicamente.
- **CORTAFUEGOS O FIREWALL**: Debe existir de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales para evitar accesos remotos indebidos a esos datos.
- **CIFRADO DE DATOS**: En caso de que sea necesario sacar los datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de usar un proceso de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD**: Se efectuará de forma periódica una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir, en caso de pérdida de la información, la recuperación de los datos personales.

GARANTIA DERECHOS DIGITALES

DERECHOS DIGITALES

LOS DERECHOS DIGITALES SON DERECHOS HUMANOS

RESOLUCIÓN 68/167 DEL CONSEJO DE DERECHOS HUMANOS DE LA ASAMBLEA GENERAL DE LAS NACIONES UNICAS, | JULIO DE 2016

FREE
%
Mercado Digital
Único Europeo
@GrupoMLT

GARANTÍA DE LOS DERECHOS DIGITALES
LOS DERECHOS EN LA ERA DIGITAL.

- El pasado 6 de diciembre de 2018, coincidiendo con el 40 aniversario de la Constitución, el BOE publicaba la nueva Ley Orgánica de Protección de Datos y **garantía de los derechos digitales**, que entraba en vigor el día siguiente. Esta ley incorpora los conocidos como derechos digitales, que hasta ahora no estaban recogidos en la legislación española.
- Los derechos digitales están recogidos en el Título X de la nueva LOPD (artículos del 79 al 97), bajo el epígrafe de "**Garantía de los derechos digitales**".
- Estos se encuentran repartidos en 4 bloques: 1) Derechos de los ciudadanos en internet, 2) Derechos de los menores y la educación, 3) Derechos relacionados con el ámbito laboral y 4) Derechos de la era digital y las comunicaciones.

LOS DERECHOS EN LA ERA DIGITAL (art. 79)

- El Título comienza con **UNA DECLARACIÓN GENERAL** de profunda implicación constitucional, pues establece que **los derechos y libertades consagrados tanto en la Constitución como en los Tratados y Convenios Internaciones en los que España sea parte, "son plenamente aplicables en internet."**
- La norma añade que **"los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar" la aplicación de tales derechos.**

Derecho a la neutralidad de Internet

Derecho de acceso universal a Internet

Derecho a la seguridad digital

Derecho a la educación digital

Protección de menores en Internet

Derecho de rectificación en Internet

Derecho a la actualización de informaciones en medios de comunicación digitales

Derechos digitales en el ámbito laboral

Derecho al olvido en Internet

Derecho de portabilidad en servicios de redes sociales y servicios equivalentes

Derecho al testamento digital

DERECHO A LA NEUTRALIDAD DE INTERNET

DERECHO A LA NEUTRALIDAD DE INTERNET (art. 80)

- Se reconoce a los **USUARIOS DE INTERNET** (concepto mucho más amplio que el de **"ciudadanos"** al que se refiere el **art. 18 de la CE**), **un derecho** cuyo contenido se concreta en **la OBLIGACIÓN de los PROVEEDORES DE SERVICIOS DE INTERNET de proporcionar "una oferta transparente de servicios sin discriminación por motivos técnicos o económicos"**

DERECHO DE ACCESO UNIVERSAL A INTERNET (art. 81)

- **NOVEDADES DE MAYOR ALCANCE SOCIAL DE LA LEY** :

❑ Que todos tienen **DERECHO A ACCEDER A INTERNET**

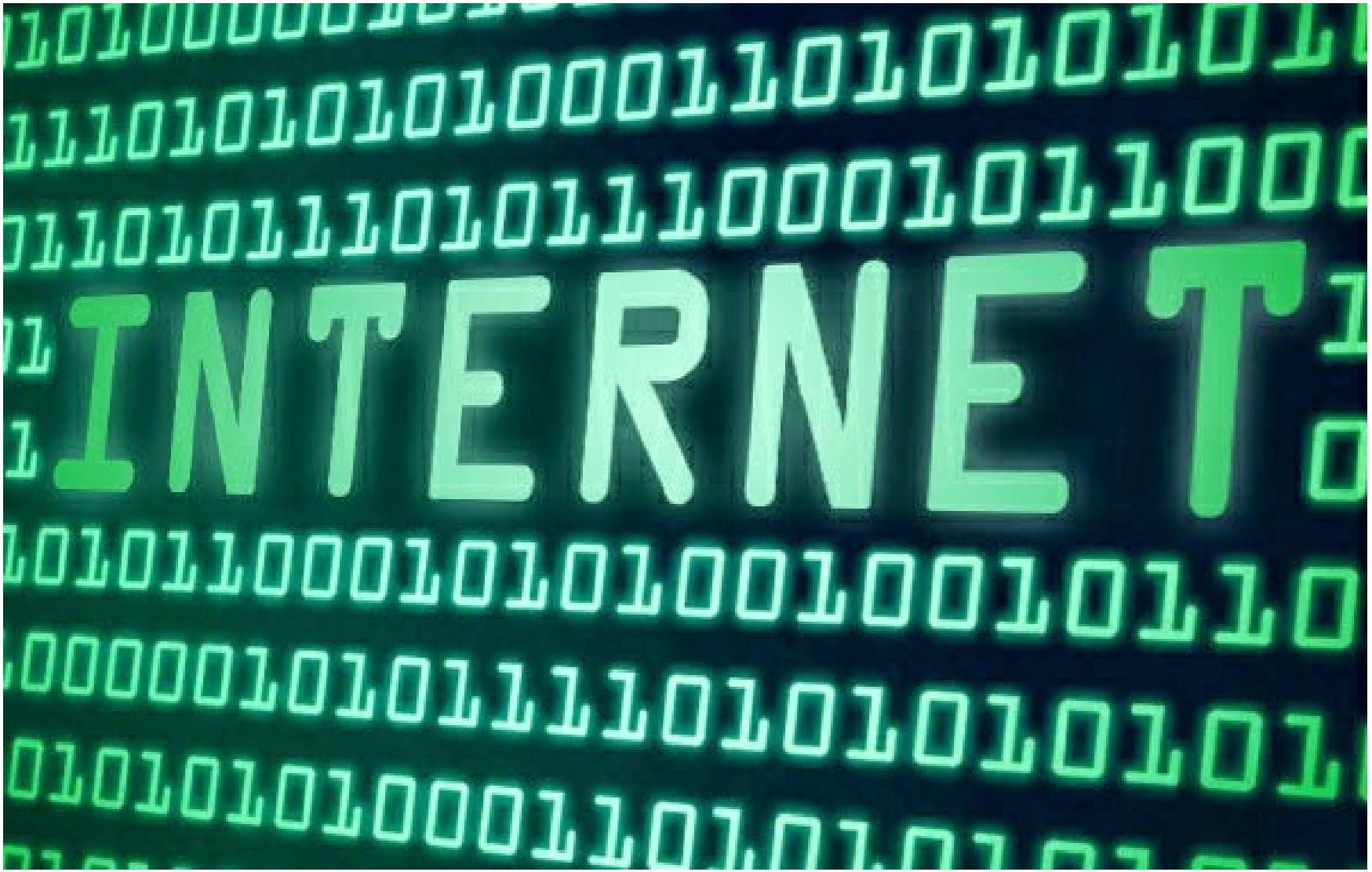
❑ Que "se garantizará" que ese acceso será "universal , asequible, de calidad y no discriminatorio para toda la población", incluidas las personas que cuenten "con necesidades especiales."

❑ Que "procurará la superación" de las brechas de género y generacional y atenderá a la realidad específica de los entornos rurales.

DERECHO DE ACCESO UNIVERSAL A INTERNET (art. 81)

- La **propuesta del acceso universal a Internet** como nuevo **DERECHO FUNDAMENTAL** a incluir en la **Constitución de 1978** y la configuración de la **NEUTRALIDAD** como principio general del Derecho de Internet se expuso con carácter pionero en nuestra doctrina por Moisés Barrio Andrés en su obra **FUNDAMENTOS DEL DERECHO DE INTERNET.**
- El contenido de este derecho debe complementarse con las **MEDIDAS DE ACCIÓN POSITIVA** que debe impulsar el Gobierno, conforme a la Ley Orgánica.

DERECHO DE ACCESO UNIVERSAL A INTERNET



Cuando los servicios que se prestan por internet afectan a Datos Personales **se aplican las dos normas.**

Publicidad por email, cookies, mensajes desde redes sociales o aplicaciones como WhatsApp, formularios de contacto web, contratación en línea, venta online, etc.

DERECHO A LA SEGURIDAD DIGITAL

DERECHO A LA SEGURIDAD DIGITAL

- Se declara que **los "usuarios" tienen derecho "a la seguridad de las comunicaciones que transmitan y reciban a través de Internet".**
- Se introduce una **OBLIGACIÓN A CARGO DE LOS PROVEEDORES DE SERVICIOS DE INTERNET**: la de informar a los usuarios de sus derechos respecto al derecho a la seguridad.

DERECHO A LA EDUCACIÓN DIGITAL

Segundo reto: Hacia una Educación digital.

Interconexión
Interdependencia

Por el buen uso de las tecnologías digitales.

La educación digital va más allá del aula, llega al hogar, al trabajo. Con la tecn la e es ex

Como docentes debemos enseñar a los educandos a utilizar adecuadamente la conectividad digital e impedir su uso excesivo, su uso impropio y su mal uso. Debemos educarlos en la prevención contra delitos cibernéticos.

No toda la sociedad tiene acceso a internet

Alumnos en situación de desventajas o, desigualdad

No solo se debe dotar a los centros de una computadora o tableta para conectar robots, jugar, entrar a Facebook o enviar correos, sino como menciona Cascal (2013), "Tienen habilitados espacios de administración, producción, adopción e intercambio sociotécnicos".

Adquisición de competencias y habilidades digitales para aprender a aprender. Formación permanente del docente y alumno.

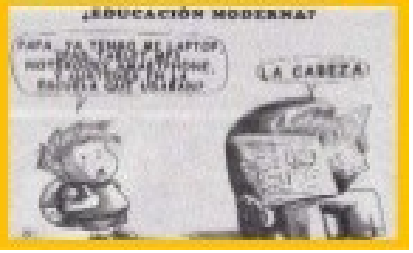
Desafíos:

- *Abatir la brecha tecnológica.*
- *Inclusión e igualdad en el mundo de la tecnología.*
- *Alfabetismo digital.*

Sociedades más conectadas, pero a la vez más alejadas, existe un abismo entre los que tienen acceso a la tecnología y los que no.

Utilizar los dispositivos móviles para que como docentes y alumnos podamos:

- ✓ Acceder a recursos educativos.
- ✓ Conectarse y comunicarse con otros.
- ✓ Crear blogs, wikis, podcasts, comunidades virtuales.
- ✓ Utilizar en beneficio del aprendizaje las diversas herramientas digitales.
- ✓ Se aprenda a ser creativo, reflexivo y autónomo.



DERECHO A LA EDUCACIÓN DIGITAL

- Garantizar que el **SISTEMA EDUCATIVO** asegure ***"la plena inserción del alumnado en la sociedad digital"*** y su aprendizaje de un uso seguro y respetuoso con ***"la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales"*** de los **medios digitales.**

DERECHO A LA EDUCACIÓN DIGITAL

Para ello:

- Se introduce **un mandato directo a todas las "Administraciones educativas"** a fin de que estas incluyan en el bloque de asignaturas de libre configuración la competencia digital anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a **las situaciones de violencia en la red.**
- A este fin **se formará adecuadamente al profesorado en competencias digitales y para la enseñanza y transmisión de los valores y derechos** referidos en el apartado anterior.
- Esa inclusión afecta igualmente **a la enseñanza universitaria**, "en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado", que deben **garantizar "la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet".**

FORMACION DIGITAL EMPLEADOS PUBLICOS

- **Las Administraciones Públicas incorporarán a los TEMARIOS DE LAS PRUEBAS DE ACCESO A LOS CUERPOS SUPERIORES,** y a aquéllos en que habitualmente se desempeñen funciones que impliquen **el ACCESO A DATOS PERSONALES** materias relacionadas **con la GARANTÍA DE LOS DERECHOS DIGITALES y en particular el de PROTECCIÓN DE DATOS.**

PROTECCIÓN DE LOS MENORES EN INTERNET

PROTECCIÓN DE LOS MENORES EN INTERNET

Se reconocen **DOS OBLIGACIONES**, que requieren de **la interpretación de los órganos judiciales** para concretar su alcance.

- 1ª.-los padres (y madres), tutores, curadores o representantes legales de los menores deben procurar ("procurarán") que los menores hagan un uso "equilibrado y responsable" de los dispositivos digitales y de los servicios de la Sociedad de la información, a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y derechos fundamentales. Este mandato es un reflejo de lo establecido en el **artículo 154 del Código Civil**, que establece que "***la patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad y con respeto a su integridad física y psicológica.***"
- 2ª.-el **Ministerio Fiscal** debe instar ("instará") las medidas cautelares y de protección previstas en la **Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor**, cuando la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes "puedan implicar" una intromisión ilegítima en sus derechos fundamentales.

DERECHO DE RECTIFICACIÓN EN INTERNET

- Se reconoce con claridad que "**TODOS TIENEN DERECHO A LA LIBERTAD DE EXPRESIÓN EN INTERNET".**
- En paralelo, "***los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación***", según "los requisitos y procedimientos previstos en la **Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación".**
- La atención a la **SOLICITUD DE RECTIFICACIÓN** dirigida contra un medio de comunicación digital debe ir acompañada de la publicación en lugar visible de sus archivos digitales ***"de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo".***

DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES

- Se reconoce el **DERECHO DE "TODA PERSONA"** a solicitar motivadamente de los **medios de comunicación digitales** la inclusión de un aviso de actualización visible junto a las noticias que le conciernan, "cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio" y, en particular, cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado por una decisión judicial posterior.

DERECHO A LA INTIMIDAD Y USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL

- Bloque de cinco artículos dedicados específicamente al **ámbito laboral** (y, en paralelo, **funcionarial o administrativo laboral**), en una relación que se complementa con lo dispuesto en las disposiciones finales 13.ª y 14.ª, que modifican respectivamente el **Estatuto de los Trabajadores y el Estatuto Básico del Empleado Público**.
- Se reconoce, en primer lugar, que tanto los trabajadores como los empleados públicos **"tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador".**
- En correlación con este derecho, se establece la **OBLIGACIÓN DE LOS EMPLEADORES** de "establecer criterios de utilización" de dichos dispositivos digitales, incluyendo la especificación de los usos autorizados y, en su caso, "la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados".
- Igualmente deben especificarse las posibilidades de acceso por el empleador al contenido de esos dispositivos digitales. De todo lo cual deben ser informados los trabajadores.
- Tales criterios de utilización deben respetar unos **ESTÁNDARES MÍNIMOS DE PRIVACIDAD** de acuerdo **"con los usos sociales y los derechos reconocidos constitucional y legalmente",** algo que parece subvertir el sistema de fuentes del Derecho previstas en el art. 1 del **Código Civil.**

DERECHO A LA DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL

DERECHO A LA DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL

- "Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital" a fin de garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.
- Las modalidades de ejercicio de este derecho "potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar" y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.
- El contenido concreto y las modalidades del ejercicio de este derecho se establece por el empleador, previa audiencia de los representantes de los trabajadores, por medio de una política interna que incluirá a los puestos directivos y prestará especial atención a los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

DERECHO A LA INTIMIDAD FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO

- Se aborda el complejo **TEMA DE LA VIDEOVIGILANCIA EN EL LUGAR DE TRABAJO**, permitiendo a los empleadores el tratamiento de las imágenes obtenidas, pero solo "para el ejercicio de las funciones de control de los trabajadores o los empleados públicos" previstas en la ley con los límites inherentes al mismo, y sin que dichos dispositivos puedan estar instalados en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos "tales como vestuarios, aseos, comedores y análogos".
- Este uso requiere la previa información, "expresa, clara y concisa", a los trabajadores y, en su caso, a sus representantes.
- La ley prevé también el caso del descubrimiento casual de la "comisión flagrante de un acto ilícito por los trabajadores", en cuyo caso "se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el art. 22.4 de esta Ley Orgánica", es decir, "un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en el Reglamento".
- Solo se admite la **UTILIZACIÓN DE SISTEMAS DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO** en caso de riesgos "relevantes" para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y respetando los principios de proporcionalidad e intervención mínima.

DERECHO A LA INTIMIDAD FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO

DERECHO A LA INTIMIDAD ANTE LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL

- Más recientes que **los SISTEMAS DE VIDEOVIGILANCIA**, los de **GEOLOCALIZACIÓN** son otros de los desarrollos tecnológicos que permiten un mayor control de la actividad de los trabajadores, que la Ley ha venido a regular.
- La Ley autoriza a los empleadores el tratamiento de los datos obtenidos "a través de **SISTEMAS DE GEOLOCALIZACIÓN"** solo para el ejercicio "de las funciones de control de los trabajadores o los empleados públicos" previstas en "su marco legal y con los límites inherentes al mismo" y previa información "expresa, clara e inequívoca" a los trabajadores o los empleados públicos y, en su caso, a sus representantes.

DERECHOS DIGITALES EN LA NEGOCIACIÓN COLECTIVA

- Como corolario a estas previsiones para el ámbito laboral, **la Ley** asume en todo caso su condición de **norma mínima**, frente a la cual **los convenios colectivos "podrán establecer garantías adicionales".**

REGISTRO HORARIO LABORAL

NUEVO REGISTRO HORARIO LABORAL

Real Decreto-ley 8/2019

CONTROL HORARIO LABORAL

- Entra en vigor el nuevo registro horario laboral: **¿cómo afecta a las empresas y a los trabajadores?**
- Las empresas tienen de plazo hasta el **12 de mayo** para adaptarse
- **Cada empresa negociará y decidirá** cómo será su registro
- El objetivo es **acabar con las horas extra sin pagar**

ACABAR CON LAS HORAS EXTRAS NO PAGADAS

El principal objetivo de la normativa ya vigente, según el Ejecutivo de Pedro Sánchez, es poner fin a las horas extras sin cobrar. Una tendencia en la economía española problemática y polémica: según la última Encuesta de Población Activa (EPA), casi 376.000 trabajadores hacen 2,96 millones de horas extra a la semana sin remunerar.

Cabe recordar que una sentencia del Tribunal Supremo (TS) de mayo de 2017 eximió a las empresas de controlar la salida y entrada de sus empleados. Sin embargo, el fallo recogía que "convendría (hacer) una reforma legislativa que clarificara la obligación de llevar un registro horario (por parte de las empresas) y facilitara al trabajador la prueba de la realización de horas extraordinarias".

PROTECCIÓN DE DATOS DE LOS MENORES EN INTERNET

- Se dirige a “los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad” y les impone la obligación de garantizar “la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales”, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.
- En los casos en que dicha publicación o difusión fuera a tener lugar a través de **servicios de redes sociales o servicios equivalentes** “deben contar con el **consentimiento del menor o sus representantes legales**”, conforme a lo prescrito en la Ley Orgánica.

Artículo 84. Protección de los menores en Internet.

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

DERECHO AL OLVIDO EN BÚSQUEDAS DE INTERNET

DERECHO AL OLVIDO EN INTERNET

DERECHO AL OLVIDO EN BÚSQUEDAS DE INTERNET

- Se reconocen **DOS MODALIDADES ESPECÍFICAS DEL DERECHO DE SUPRESIÓN, O DERECHO AL OLVIDO**, regulados en los arts. 17 del RGPD y 15 de la Ley Orgánica 3/2018, para el ámbito de internet.
- En el art. 93 se establece **UN DERECHO DE "TODA PERSONA" FRENTE A LOS MOTORES DE BÚSQUEDA EN INTERNET** y en el art. 94 **FRENTE A LOS "SERVICIOS DE REDES SOCIALES Y SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN EQUIVALENTES".**
- Los **MOTORES DE BÚSQUEDA** deben eliminar de las listas de resultados "que se obtuvieran tras una búsqueda efectuada a partir de su nombre", de los enlaces publicados que contuvieran "información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo", todo ello teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
- Es decir, se trata de un derecho ejercible frente a **UN BUSCADOR**, pero no frente a un medio de comunicación, y que "no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho".

OLVIDO EN LAS REDES SOCIALES

Artículo 94. Derecho al olvido en servicios de redes sociales y servicios equivalentes.

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

DERECHO AL OLVIDO EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES

- Se reconoce el derecho de “toda persona” a que sean suprimidos, “a su simple solicitud”, los datos personales publicado en las redes sociales, ya los hubiera facilitado ella misma, ya “hubiesen sido facilitados por terceros”, en este caso “cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo” o cuando las “circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio”.
- En coherencia con lo dispuesto en el RGPD, que establece que el mismo no se aplica al tratamiento de datos personales “efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas”, y con el Cdo. 18 que indica que entre esas actividades cabe incluir “la actividad en las redes sociales”, se exceptúan también de lo dispuesto en el art. 94 de la Ley Orgánica “los datos que hubiesen sido facilitados por personas físicas” en el ejercicio de tales actividades.
- Se recoge una mención específica para el caso de que el derecho se ejercitase “por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad”. En estos casos, el prestador “deberá proceder sin dilación a su supresión por su simple solicitud”.

Diseño y fotografía: Sonsoles Valero
Insta
LA INMORTALIDAD DE LA VIDA DIGITAL.
DERECHO E IDENTIDAD DIGITAL POST MORTEM
Ricardo Oliva León

DERECHO DE PORTABILIDAD

PORTABILIDAD

Artículo 95. Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

DERECHO DE PORTABILIDAD EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES

- Se reconoce una modalidad específica de un derecho para un ámbito concreto.
- En este caso se trata del **DERECHO A LA PORTABILIDAD DE LOS DATOS QUE LE INCUMBAN** y que haya facilitado a un responsable de tratamiento, y cuyo ejercicio, se realizará "de acuerdo con lo establecido" para de los usuarios de servicios de redes sociales y de servicios equivalentes.
- Dichos usuarios "tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios", así como a que tales los prestadores "los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible".

MI LEGADO DIGITAL

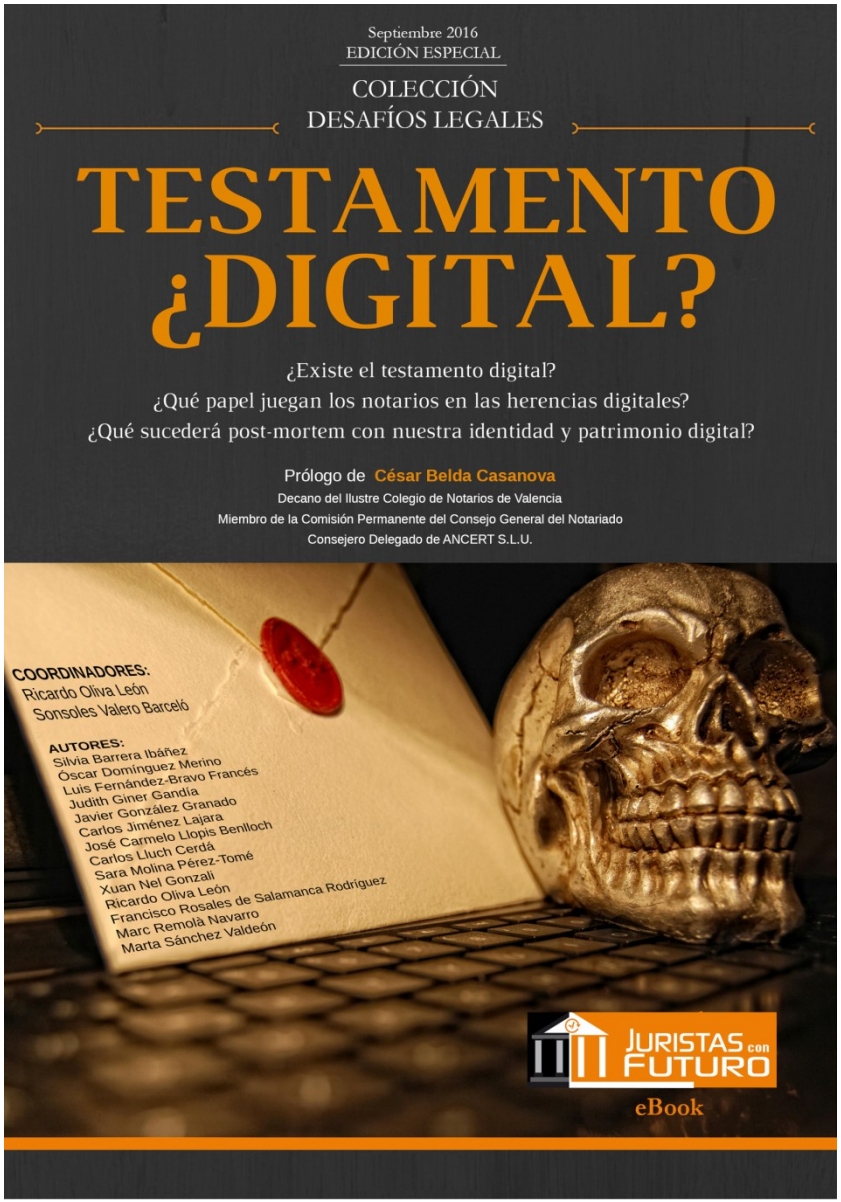
Lo Mejor de Ti, también Online

TESTAMENTO DIGITAL

Defiende tus derechos

al honor, la imagen, la salud,
la intimidad, la privacidad,
la reputación online, al olvido
y al secreto de las comunicaciones.

DERECHO AL TESTAMENTO DIGITAL



DERECHO AL TESTAMENTO DIGITAL

- La Ley Orgánica establece que la misma no es de aplicación “a los tratamientos de datos de personas fallecidas”. Pero fija los criterios conforme a los cuales las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, pueden acceder a los datos personales de aquél.
- No se regula una nueva forma testamentaria, diferente de las ya previstas en el Código Civil. Más bien viene a prever un contenido específico de las disposiciones testamentarias que puede realizar una persona, referidas a un tipo concreto de “bienes” como son el contenido de la información relativa a la misma “gestionados por prestadores de servicios de la sociedad de la información”.
- “las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión”, siempre que la persona fallecida no lo hubiese prohibido expresamente (o así lo establezca una ley) y si bien dicha prohibición “no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto”.
- La Ley Orgánica remite al desarrollo reglamentario “los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos”.

Epa!
TESTAMENTO DIGITAL
¿Hay Redes Sociales
después de la muerte?

POLÍTICAS DE IMPULSO DE LOS DERECHOS DIGITALES

- El Gobierno de la Nación, en colaboración con **LAS COMUNIDADES AUTÓNOMAS**, debe elaborar dos documentos:

❑- **UN "PLAN DE ACCESO A INTERNET**" orientado a superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos (mediante, entre otras medidas, un bono social de acceso a Internet; impulsar la existencia de espacios de conexión de acceso público y fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

❑**- UN "PLAN DE ACTUACIÓN**" dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

Artículo 97. Políticas de impulso de los derechos digitales.

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías

Certificación del **Esquema Nacional de Seguridad**

ens Esquema Nacional de Seguridad

Adaptación de la LOPD al **RGPD**

ens Esquema Nacional de Seguridad

CERTIFICACIÓN DE CONFORMIDAD CON EL

ens Esquema Nacional de Seguridad

Categoría ALTA

RD 3/2010

MEDIDAS DE SEGURIDAD EN EL ÁMBITO DEL SECTOR PÚBLICO

- El **Esquema Nacional de Seguridad** incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el Reglamento (UE) 2016/679.
- Los responsables enumerados en la ley orgánica deben aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el **Esquema Nacional de Seguridad**, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.
- En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

PROTECCIÓN DE DATOS Y TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

- La publicidad activa y el acceso a la información pública regulados en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la ley orgánica.

CÓMPUTO DE PLAZOS

Los **plazos establecidos en el Reglamento (UE) 2016/679** o en la **ley orgánica,** con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se rigen por las siguientes **REGLAS:**

- Cuando **los plazos se señalen por días**, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.
- Si **el plazo se fija en semanas**, concluye el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.
- Si **el plazo se fija en meses o años**, concluye el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entiende que el plazo expira el último día del mes.
- Cuando **el último día del plazo sea inhábil**, se entiende prorrogado al primer día hábil siguiente.

AUTORIZACIÓN JUDICIAL EN RELACIÓN CON DECISIONES DE LA COMISIÓN EUROPEA EN MATERIA DE TRANSFERENCIA INTERNACIONAL DE DATOS.

AUTORIZACIÓN JUDICIAL EN RELACIÓN CON DECISIONES DE LA COMISIÓN EUROPEA EN MATERIA DE TRANSFERENCIA INTERNACIONAL DE DATOS.

- 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 pueden 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 los siguientes supuestos.

DESTINATARIO DECLARADO DE NIVEL ADECUADO POR LA COMISIÓN EUROPEA

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:

- **Suiza**. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000
- **Canadá**. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos
- **Argentina**. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003
- **Guernsey**. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
- **Isla de Man**. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
- **Jersey**. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
- **Islas Feroe**. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
- **Andorra**. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
- **Israel**. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
- **Uruguay**. Decisión 2012/484/UE, de la Comisión de 21 de agosto de 2012.
- **Nueva Zelanda**. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012
- **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.
- **Japón**. Decisión de 23 de enero de 2019.

A FALTA DE DECISIÓN DE ADECUACIÓN, CON LAS SIGUIENTES GARANTÍAS

- 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 que siguen siendo válidas
  - Decisión 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales entre responsables del tratamiento a un tercer país y
  - Decisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países
  - Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo
- Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión
- Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados
- Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

A FALTA DE DECISIÓN DE ADECUACIÓN Y DE GARANTÍAS

A FALTA DE DECISIÓN DE ADECUACIÓN Y DE GARANTÍAS ADECUADAS ÚNICAMENTE SE PODRÁN REALIZAR SI SE CUMPLE ALGUNA DE LAS CONDICIONES SIGUIENTES:

- El interesado haya dado explícitamente su consentimiento
- La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
- La transferencia sea necesaria por razones importantes de interés público
- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
- La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento
- La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

CUÁNDO SE NECESITA UNA AUTORIZACIÓN EXPRESA

SE NECESITARÁ AUTORIZACIÓN EXPRESA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS CUANDO LAS GARANTÍAS ADECUADAS SE APORTEN MEDIANTE:

- ❑ cláusulas contractuales entre el responsable o el encargado y el responsable, y el encargado y subencargado, que no hayan sido adoptadas por la Comisión Europea o
- ❑ disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

- Las **autorizaciones otorgadas por la Agencia Española de Protección de Datos** previamente a la aplicación del RGPD seguirán siendo válidas.

NORMAS CORPORATIVAS VINCULANTES (BCR)

- Las normas corporativas vinculantes (o BCR por sus siglas en inglés) son " *las 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*".
- Los grupos empresariales son aquellos" *constituidos por una empresa que ejerce el control y sus empresas controladas*".
- 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 RGPD.
- Los grupos empresariales interesados en la elaboración de normas corporativas vinculantes pueden solicitar información en la siguiente dirección de correo electrónico: rgpd@agpd.es.

INCORPORACIÓN DE DEUDAS A SISTEMAS DE INFORMACIÓN CREDITICIA

- Millones de españoles figuran en alguna **LISTA DE MOROSOS**, una inclusión que les puede generar algún problema a la hora de acudir a un banco a solicitar un crédito personal, por ejemplo. Solo en los ficheros de la **Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) Y EQUIFAX** se encuentran datos de más de 4 millones de ciudadanos que pueden tener algún tipo de deuda.
- Un importante porcentaje de los afectados son consumidores que **no han pagado alguna factura telefónica** y pasan a aparecer automáticamente en estos listados, pero otros han sido víctimas de una suplantación de identidad

INCORPORACIÓN DE DEUDAS A SISTEMAS DE INFORMACIÓN CREDITICIA

- En el aspecto económico hay **dos novedades importantes**.
- La primera afecta a la citada incorporación de **deudas a sistemas de información crediticia**, es decir, a los famosos listados de morosos.
- Así, no se podrán incorporar a estos sistemas de datos crediticios a aquellos particulares o empresas que adeuden una cuantía inferior a **50 euros**.
- Actualmente, cualquier español **con un euro de deuda** de cualquier tipo puede ser incluido en estos listados de morosos.

INCORPORACIÓN DE DEUDAS A SISTEMAS DE INFORMACIÓN CREDITICIA

INCORPORACIÓN DE DEUDAS A SISTEMAS DE INFORMACIÓN CREDITICIA.

- La **inclusión de datos de deudores en sistemas de información crediticia** (**LISTADOS DE MOROSOS**) está sujeta a requisitos relativos a los datos personales, a los acreedores y a las entidades que mantienen el sistema de información crediticia, así como a quienes los consultan.
- Las entidades que mantengan el sistema de información crediticia y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, son considerados como corresponsables del tratamiento.
- La presunción sobre la licitud del tratamiento de datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito no es aplicable cuando se trate con fines de perfilado del deudor.

SISTEMAS DE INFORMACIÓN CREDITICIA

Salvo prueba en contrario, **se presume lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia** cuando se cumplan los siguientes requisitos:

- ❑Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.
- ❑Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.
- ❑Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.
- ❑La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.
- ❑ Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.
- ❑Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.
- ❑Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.
- ❑Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

SISTEMAS DE INFORMACIÓN CREDITICIA

- Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tienen la condición de corresponsables del tratamiento de los datos.
- Corresponde al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.
- La presunción de licitud del tratamiento de datos personales no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema, a informaciones adicionales a las dinerarias, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo **un perfilado del mismo**, en particular mediante la aplicación de técnicas de calificación crediticia.

IDENTIFICACIÓN DE LOS INTERESADOS EN LAS NOTIFICACIONES POR MEDIO DE ANUNCIOS Y PUBLICACIONES DE ACTOS ADMINISTRATIVOS.

- Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identifica al mismo mediante su nombre y apellidos, añadiendo 4 cifras numéricas aleatorias del DNI, número de identidad de extranjero, pasaporte o documento equivalente.
- Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.
- Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
- Cuando el afectado careciera de cualquiera de los documentos anteriores, se identifica al afectado únicamente mediante su nombre y apellidos.
- En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
- A fin de prevenir **riesgos para víctimas de violencia de género**, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

POTESTAD DE VERIFICACIÓN DE LAS ADMINISTRACIONES PÚBLICAS DE LOS DATOS PERSONALES DE LOS CIUDADANOS

POTESTAD DE VERIFICACIÓN DE LAS ADMINISTRACIONES PÚBLICAS DE LOS DATOS PERSONALES DE LOS CIUDADANOS

- Los **ÓRGANOS Y ORGANISMOS DEL SECTOR PÚBLICO** pueden verificar, sin necesidad de solicitar consentimiento del interesado, la exactitud de los datos personales manifestados por los ciudadanos que obren en poder de los órganos y organismos del Sector Público.

PRÁCTICAS AGRESIVAS EN MATERIA DE PROTECCIÓN DE DATOS

- Actuar con intención de suplantar la identidad de la AEPD o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.
- Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la AEPD o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.
- Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.
- Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.
- Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la AEPD o las autoridades autonómicas de protección de datos.

TRATAMIENTOS DE DATOS DE SALUD

TRATAMIENTOS DE DATOS DE SALUD

Se encuentran amparados en **el Reglamento (UE) 2016/679** los **TRATAMIENTOS DE DATOS RELACIONADOS CON LA SALUD Y DE DATOS GENÉTICOS** que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

- La Ley 14/1986, de 25 de abril, General de Sanidad.
- La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
- La Ley 14/2007, de 3 de julio, de Investigación biomédica.
- La Ley 33/2011, de 4 de octubre, General de Salud Pública.
- La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.
- El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

TRATAMIENTOS DE DATOS DE SALUD

EL TRATAMIENTO DE DATOS EN LA INVESTIGACIÓN EN SALUD SE REGIRÁ POR LOS SIGUIENTES CRITERIOS:

- El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.
- Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.
- Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.
- En tales casos, los responsables deberán publicar la información establecida por el Reglamento (UE) de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.
- Para estos tratamientos, se requerirá informe previo favorable del comité de ética de la investigación.
- Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

TRATAMIENTOS DE DATOS DE SALUD

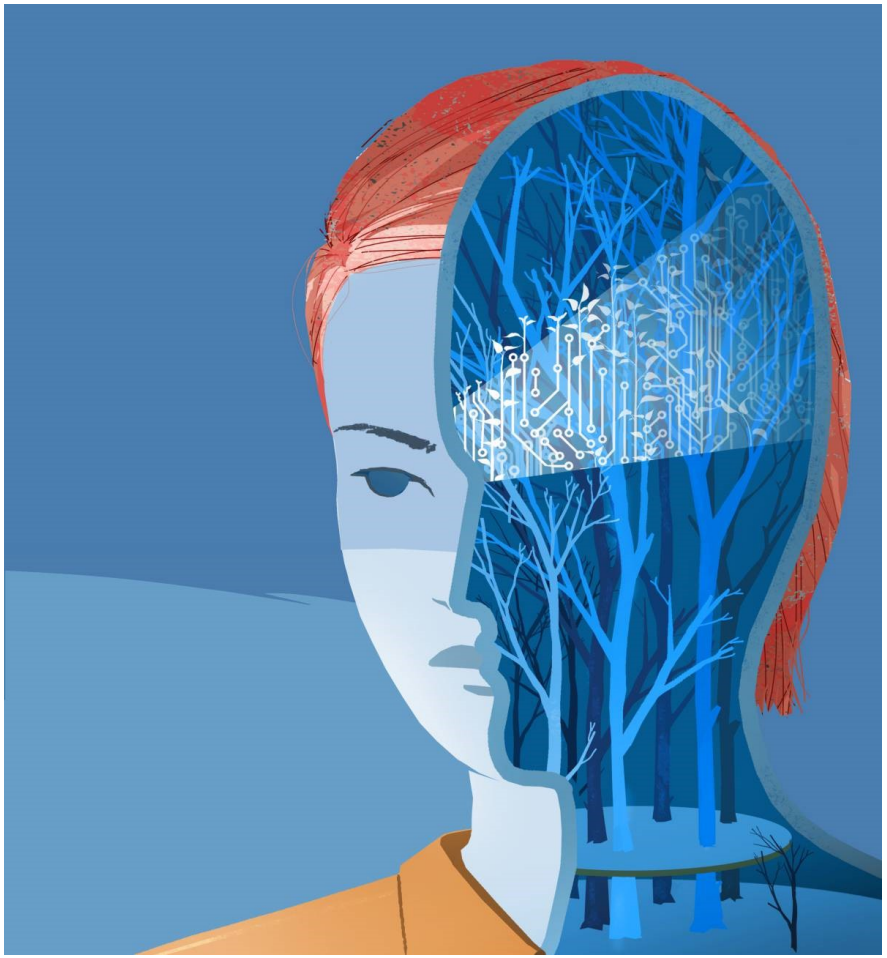
El **uso de DATOS PERSONALES SEUDONIMIZADOS con fines de investigación en salud pública y biomédica** requiere:

- 1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.
- 2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:
- i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
- ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.
- Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.
- e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, podrán excepcionarse los derechos de los afectados previstos el Reglamento (EU) cuando:
- 1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.
- 2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.
- 3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

TRATAMIENTOS DE DATOS DE SALUD

- f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:
- 1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.
- 2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.
- 3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.
- 4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.
- g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.
- En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.
- h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

TRATAMIENTOS DE DATOS DE SALUD



PUBLICACIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO DEL ÓRGANO U ORGANISMO DEL SECTOR PÚBLICO

- Los órganos y organismos del Sector Público quedan obligados a publicar en su web el inventario de las actividades de tratamiento de datos personales que realizan, identificando quién trata los datos, con qué finalidad y qué base jurídica legitima ese tratamiento.
- En el **Portal de la Transparencia** se recoge de forma centralizada toda la información de los **REGISTROS DE ACTIVIDADES DE TRATAMIENTO.**

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

OBLIGACIÓN DE INFORMACIÓN A LOS CIUDADANOS SOBRE EL EJERCICIO DE SUS DERECHOS.

- Los órganos y organismos del Sector Público quedan obligados a incluir en su página web información clara y precisa destinada a los administrados sobre el ejercicio de los derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, así como a la portabilidad y oposición.

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

NUEVA REGULACIÓN DE LA APORTACIÓN DE DOCUMENTACIÓN POR PARTE DE LOS CIUDADANOS: MODIFICACIÓN DEL ARTÍCULO 28 DE LA LEY 39/2015

- Ya la ley 30/1992 reconocía a los administrados el derecho a no aportar a los procedimientos administrativos los documentos que obrasen en poder de la Administración, o que hubiesen sido elaborados por ésta. La base jurídica del tratamiento de los datos personales por la Administración era el consentimiento del administrado, que se entendía tácitamente concedido si el interesado no se oponía expresamente.
- Tanto el Reglamento General de Protección de Datos como la nueva Ley Orgánica eliminan la necesidad de recabar el consentimiento, ni siquiera tácito, del ciudadano, al establecer como base jurídica legitimadora principal del tratamiento de datos personales por órganos y organismos del Sector Público el cumplimiento de una misión en interés público o, particularmente, el ejercicio de poderes públicos.
- Asimismo, la nueva redacción otorgada por la Ley Orgánica al artículo 28 de la Ley 39/2015 reconoce al interesado la posibilidad de oponerse a que órganos y organismos del Sector Público consulten o recaben los citados documentos, pero en ese caso el administrado deberá aportarlos necesariamente para que la Administración pueda conocer que concurren en él los requisitos establecidos por la norma. En caso contrario no podrán estimar su solicitud, precisamente porque no habría demostrado los requisitos requeridos.
- En todo caso, dicho derecho de oposición no juega en los casos de potestades de verificación o inspección.

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

NOTIFICACIÓN DE ACTOS ADMINISTRATIVOS: IDENTIFICACIÓN DE LOS CIUDADANOS

- La nueva Ley impide el uso conjunto apellidos, nombre y número completo del documento de identificación oficial de las personas en aquellos actos administrativos que vayan a ser objeto de publicación o notificación por medio de anuncios.
- A partir de la entrada en vigor de la Ley Orgánica:
- Cuando un acto administrativo se deba publicar se identificará a la persona mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su documento identificativo oficial.
- Cuando se trate de notificaciones por medio de anuncios se identificará a la persona exclusivamente con el número de su documento identificativo.
- En ambos casos, cuando la persona carezca de documento identificativo se la identificará sólo mediante su nombre y apellidos.

COMUNICACIÓN DE DATOS PERSONALES DE LOS ADMINISTRADOS A SUJETOS PRIVADOS

- Los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten:
  - o bien cuando cuenten con el consentimiento de los administrados.
  - o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

DESIGNACIÓN DE UN DELEGADO DE PROTECCIÓN DE DATOS (DPD) Y COMUNICACIÓN DE LA DESIGNACIÓN A LA AEPD

- Los órganos y organismos del Sector Público tienen obligación de designar un Delegado de Protección de Datos que cuente con la debida cualificación, de garantizarle los medios necesarios para el ejercicio de sus funciones y de notificar la designación a la AEPD para su inclusión en el Registro público de Delegados de Protección de Datos.
- El Delegado de Protección de Datos no tiene responsabilidad a título personal, por este mero hecho, por las posibles infracciones en materia de protección de datos cometidas por su organización.

INTERVENCIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA RESOLUCIÓN DE RECLAMACIONES EN EL SECTOR PÚBLICO

- El Delegado de Protección de Datos del órgano u organismo del Sector Público debe recibir las reclamaciones que les dirijan los administrados, cuando opten por esta vía antes de plantear una reclamación ante la AEPD, y comunicará la decisión adoptada al administrado en el plazo máximo de dos meses.
- Asimismo, el Delegado de Protección de Datos deberá recibir las reclamaciones que la AEPD decida trasladarle con carácter previo al inicio de un expediente sancionador. El Delegado debe comunicar la decisión adoptada al administrado y a la AEPD en el plazo máximo de un mes.
- De esta forma, con carácter general, si el Delegado de Protección de Datos consigue que el responsable resuelva por cualquiera de estas dos vías la reclamación, y sin perjuicio de que el interesado posteriormente se dirija a la AEPD, no se iniciaría expediente de declaración de infracción a esa Administración Pública.

LAS ADMINISTRACIONES PÚBLICAS NO PAGARÁN MULTAS Y SOLO SERÁN APERCIBIDAS SI VULNERAN LA LEY DE PROTECCIÓN DE DATOS

- Cuando los **RESPONSABLES O ENCARGADOS DE LAS ADMINISTRACIONES PÚBLICAS** cometiesen alguna infracción contra la protección de datos, desde las más graves a las más leves, “la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido”.

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

- **MAYOR TRANSPARENCIA DE LAS SANCIONES IMPUESTAS AL SECTOR PÚBLICO**

❑Las infracciones cometidas por los **ÓRGANOS Y ORGANISMOS DEL SECTOR PÚBLICO** serán sancionadas con **un apercibimiento con medidas correctoras** y no tendrán sanción económica.

❑La **resolución sancionadora de la AEPD** identificará el cargo responsable de la infracción, se notificará al infractor, a su superior jerárquico, al Defensor del Pueblo y se publicará en la página web de la AEPD y en el diario oficial correspondiente.

❑La resolución sancionadora puede proponer al órgano u organismo la iniciación de actuaciones disciplinarias, cuya resolución debe ser comunicada por el órgano u organismo del Sector Público a la AEPD.

❑Las infracciones sean imputables a **autoridades y directivos del Sector Público** y se acredite la existencia de informes técnicos o recomendaciones que no hubieran sido atendidos por estos, la resolución sancionadora incluirá **una amonestación** con la identificación del cargo responsable y se publicará en el diario oficial correspondiente.

¿Peor que las sanciones económicas...?

Noticias de actualidad | Actualidad

11/04/2018 16:54:54 | IRENE CORTÉS | #YOCUMPLORGPD

La AEPD atribuye una infracción grave al Ministerio de Justicia por la brecha de seguridad de la LexNET

La Agencia Española de Protección de Datos (AEPD) ha hecho pública su Resolución en la que confirma que **el Ministerio de Justicia ha cometido una infracción tipificada como grave** en la Ley Orgánica de Protección de Datos (LOPD) a causa de la **brecha de seguridad de la plataforma LexNET** que permitió a los usuarios acceder a los buzones personales de terceros. También queda demostrado, que **el fallo no afectó a ficheros jurisdiccionales ni a expedientes completos.**

HOSPITAL VIRGEN DE LA LUZ

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS
REFERÈNDUM

Ley Orgánica 3/2018, de 5 de diciembre,
NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

TRATAMIENTO DE DATOS PERSONALES EN LA NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

- Las autoridades públicas, los equipos de respuesta a emergencias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de seguridad pueden tratar los datos personales contenidos en las notificaciones de incidentes de seguridad exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta, adoptando siempre las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo

Ley Orgánica 3/2018, de 5 de diciembre,
NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

REGISTROS DE PERSONAL DEL SECTOR PÚBLICO: LEGITIMACIÓN DEL TRATAMIENTO

- La nueva Ley Orgánica establece que la base legitimadora del tratamiento de datos personales que realizan los registros de personal del sector público es el ejercicio de potestades públicas.
- Estos registros pueden tratar los datos personales que sean estrictamente necesarios para el cumplimiento de sus fines relativos a infracciones y condenas penales e infracciones y sanciones administrativas, de los que deberán ser informados de manera expresa, clara e inequívoca.

Ley Orgánica 3/2018, de 5 de diciembre,
NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

DERECHOS DE LOS EMPLEADOS PÚBLICOS: MAYOR INTIMIDAD

- La Ley Orgánica garantiza el derecho a la intimidad de los empleados públicos en el lugar de trabajo frente al uso de dispositivos de videovigilancia y de grabación de sonidos, así como frente al uso de los dispositivos digitales y sistemas de geolocalización.

Ley Orgánica 3/2018, de 5 de diciembre,
NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

ADAPTACIÓN A LA LEY ORGÁNICA DE LOS CONTRATOS DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

- Los contratos de encargo de tratamiento de datos personales entre los órganos y organismos del Sector Público (como responsables) y otros órganos u organismos del sector público o terceros (como encargados de tratamiento) suscritos antes del **25 de mayo de 2018** mantendrán su vigencia como máximo hasta **el 25 de mayo de 2022.**

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

TRATAMIENTO DE DATOS PERSONALES POR CONCESIONARIOS DE SERVICIOS PÚBLICOS

- Los **órganos y organismos del Sector Público** mantendrán el control sobre los datos personales de los usuarios de los servicios públicos aunque haya finalizado la vigencia del contrato de concesión de servicios.
- En el Sector Público, un concesionario de servicios, encargado del tratamiento de datos personales, no se convierte nunca en responsable aunque establezca relaciones con las personas a cuyos datos ha accedido en virtud de la prestación del servicio.

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

EDUCACIÓN PARA LA DIGITALIZACIÓN

- **El Gobierno** remitirá en el plazo de un año desde la entrada en vigor de la Ley Orgánica un **PROYECTO DE LEY dirigido a garantizar un uso de los medios digitales que sea seguro y adecuado.**
- **Las Comunidades Autónomas** dispondrán del mismo plazo para incluir en los currículos los contenidos precisos para garantizar **la plena inserción del alumnado en la sociedad digital** y asegurar **una formación adecuada de todo el personal docente.**

DERECHO A LA EDUCACIÓN DIGITAL.
Garantía de derechos digitales.
• Plena inserción del **alumnado** en el uso seguro de medios digitales respetando valores constitucionales y derechos fundamentales como intimidad.
• Formación al **profesorado** en competencias digitales y protección de derechos digitales.
• Los **planes universitarios** sobre uso y seguridad de los derechos en los medios digitales.
#AhoraDerechosDigitales
Hacer País.
PSOE
Somos la Izquierda

Ley Orgánica 3/2018, de 5 de diciembre, NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

TRATAMIENTO DE DATOS PERSONALES EN INVESTIGACIÓN SANITARIA

- La nueva Ley Orgánica flexibiliza el **TRATAMIENTO DE DATOS PARA LA INVESTIGACIÓN EN SALUD:**

❑amplía las finalidades para las que se puede otorgar el consentimiento al tratamiento,

❑recoge la posibilidad de reutilizar la información sobre la que se ya se haya prestado consentimiento con anterioridad,

❑recoge el uso de datos pseudonimizados como una opción para facilitar la investigación sanitaria incluyendo garantías para evitar la reidentificación de los afectados,

❑regula las garantías de este tratamiento, incluyendo la intervención de **los Comités de Ética de la Investigación** o, en su defecto, del **Delegado de Protección de Datos** o de **un experto en protección de datos personales.**

ESQUEMA NACIONAL DE SEGURIDAD

TRANSPARENCIA, BUEN GOBIERNO Y PROTECCIÓN DE DATOS

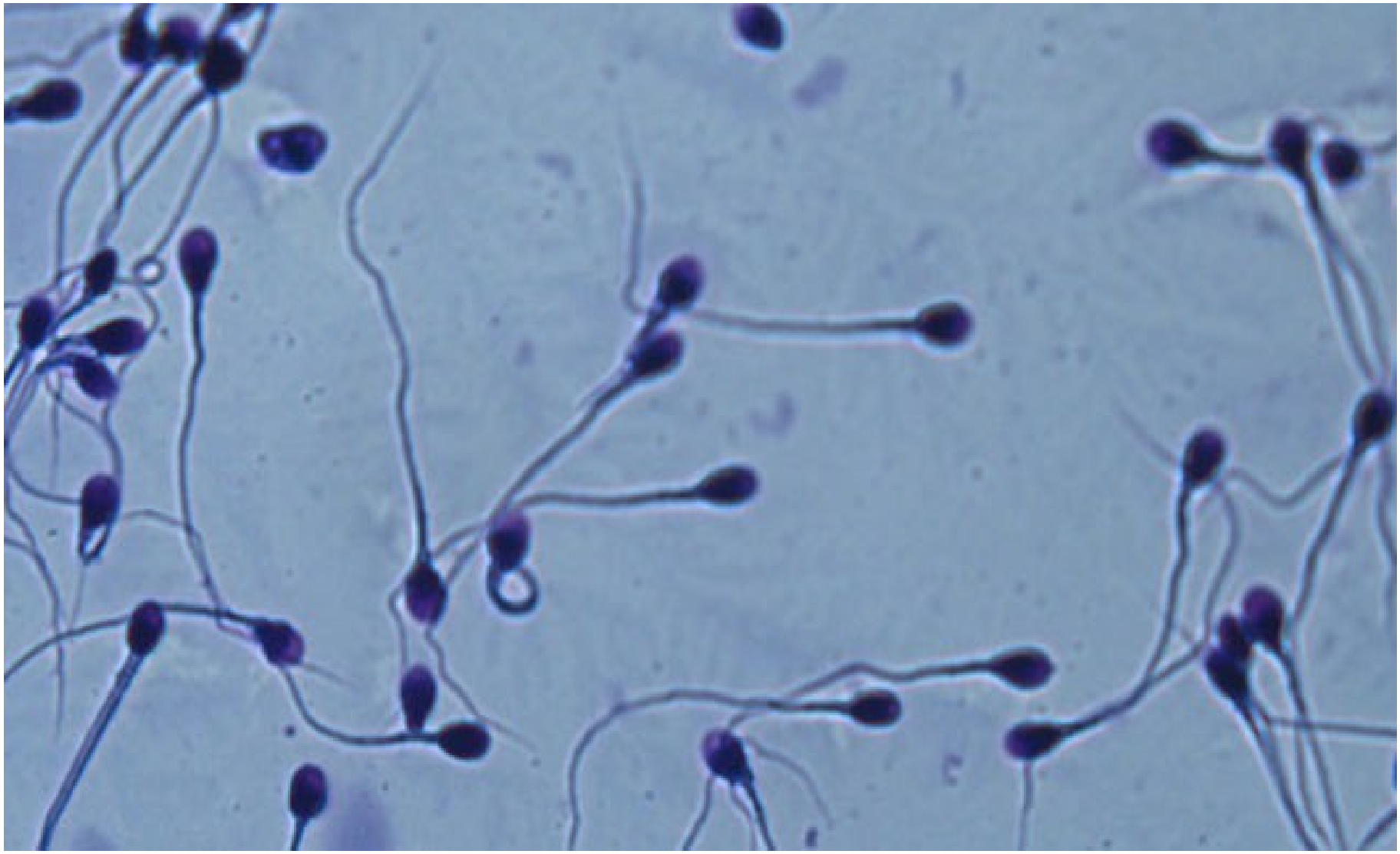
- La **Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno** incrementa y refuerza la **TRANSPARENCIA EN LA ACTIVIDAD PÚBLICA**, por medio de obligaciones de publicidad activa para todas las Administraciones y entidades públicas, reconoce y garantiza el acceso a la información y establece las obligaciones de buen gobierno que deben cumplir los responsables públicos, así como las consecuencias jurídicas derivadas de su incumplimiento.

TRANSPARENCIA, BUEN GOBIERNO Y PROTECCIÓN DE DATOS

- Nos encontramos ante una **ley esencial y vertebradora** de todo **Estado social y democrático de Derecho**, pero.

- ❑ **¿QUÉ RELACIÓN GUARDA EL DERECHO DE ACCESO A LA INFORMACIÓN CON LA PROTECCIÓN DE DATOS?**
- ❑ **¿CUÁNDO TENEMOS DERECHO A ACCEDER A LA INFORMACIÓN PÚBLICA?**
- ❑ **¿CÓMO TRAMITO LA SOLICITUD?**
- ❑ **¿CUÁLES SON LAS CAUSAS DE INADMISIÓN?**
- ❑ **¿CÓMO PUEDO IMPUGNAR UNA DENEGACIÓN DE ACCESO?**

REPRODUCCIÓN HUMANA ASISTIDA



PROTECCIÓN DE DATOS Y PREVENCIÓN DE DELITOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

28 DE ENERO

DÍA EUROPEO
DE LA PROTECCIÓN DE DATOS

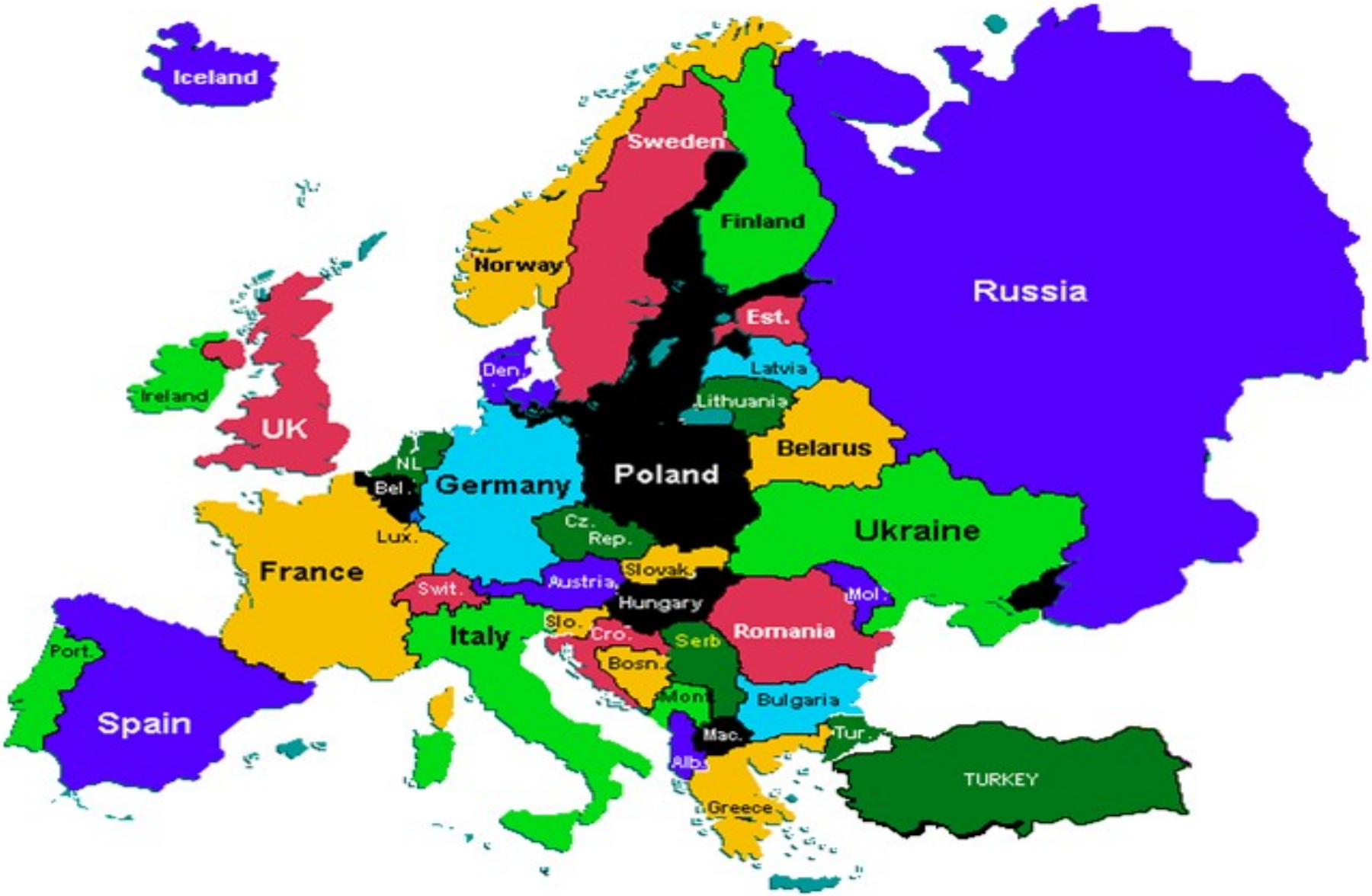
TIENES UN DERECHO FUNDAMENTAL A LA PROTECCIÓN DE TUS DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

¡CONÓCELO!

NEWS
FAKE

II
III
IV
70%
50%
1 2 3 4 5 6 7 8 9 10
12
11
10


Iceland
Sweden
Finland
Norway
Russia
Est.
Latvia
Lithuania
Den.
Ireland
UK
Belarus
NL
Bel.
Germany
Poland
Ukraine
Cz. Rep.
Lux.
France
Slovak.
Swit.
Austria
Hungary
Mol.
Romania
Slo.
Cro.
Serb
Italy
Port.
Bosn.
Mont.
Bulgaria
Spain
Mac.
Tur.
Alb.
TURKEY
Greece