G CONSELLERIA
O PRESIDÈNCIA
I DIRECCIÓ ADVOCACIA
B COMUNITAT AUTÒNOMA

# V JORNADAS SOBRE EL CONTROL JURISDICCIONAL DE LAS ADMINISTRACIONES PÚBLICAS

## *La protección de datos en las actuaciones administrativas*

Palma de Mallorca, 22 de marzo de 2019

**José Luis Piñar Mañas**
Catedrático de Derecho Administrativo
Abogado

**PROTECCION DE DATOS:**

**PRESUPUESTOS**

**TRATAMIENTO DE DATOS DE CARÁCTER**

**PERSONAL**

**PERSONAS FISICAS, INDIVIDUALIZADAS O INDIVIDUALIZABLES**

**Personas fallecidas, personas jurídicas, tratamiento para uso personal o doméstico**

**PROTECCION DE DATOS COMO DERECHO FUNDAMENTAL**

**CARTA EUROPEA DE DERECHOS HUMANOS**

**SSTC 290 y 292/2000**

**OTRAS NORMAS**

**PODER DE DISPOSICION**

**SOBRE LOS PROPIOS DATOS**

**DE CARÁCTER PERSONAL**

**DISTINTO DEL DERECHO A LA INTIMIDAD**

**PROTECCION DE DATOS COMO DERECHO FUNDAMENTAL**

**PRINCIPIOS**

**TRANSPARENCIA**
**LICITUD**
**FINALIDAD**
**CALIDAD DEL DATO**
**SEGURIDAD**
**CONTROL INDEPENDIENTE**
**RESPONSABILIDAD PROACTIVA**
**PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO**

**REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (CAPITULO II)**

**LOPDGDD (TITULO II)**

# MARCO NORMATIVO DE LA PROTECCION DE DATOS EN ESPAÑA

**ART. 18.4 CONSTITUCION**
**ESTATUTOS DE AUTONOMIA**
**REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE**
**LOPDGDD**
**LEY 39/2015**
**LEYES DE TRANSPARENCIA**
**LCSP**
**LOPJ**
**LEY 34/2002 (LSSI)**
**LEY 9/2014 (LGT)**
**LEYES AUTONOMICAS**
***INSTRUCCIONES Y CIRCULARES DE LA AEPD***
**OTRAS NORMAS SECTORIALES**

- **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 (DOUE L 119, de 4-5-2016).

# ADAPTACIÓN DE LA LEGISLACIÓN ESPAÑOLA AL RGPD

## Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales

Título I. Disposiciones generales
Título II. Principios de protección de datos
Título III. Derechos de las personas
- CAPITULO I. Transparencia e información
- CAPITULO II. Ejercicio de los derechos

Título IV. Disposiciones aplicables a tratamientos concretos
Título V. Responsable y encargado del tratamiento
- CAPITULO I. Disposiciones generales. Medidas de responsabilidad activa.
- CAPITULO II. Encargado del tratamiento
- CAPITULO III. Delegado de protección de datos
- CAPITULO IV. Códigos de conducta y certificación

Título VI. Transferencias internacionales de datos

Título VII. Autoridades de protección de datos

- CAPITULO I. La Agencia Española de Protección de Datos
  - SECCIÓN 1ª DISPOSICIONES GENERALES
  - SECCIÓN 2ª POTESTADES DE INVESTIGACIÓN Y PLANES DE AUDITORÍA PREVENTIVA
  - SECCIÓN 3ª OTRAS POTESTADES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
- CAPITULO II. Autoridades autonómicas de protección de datos
  - SECCIÓN 1ª DISPOSICIONES GENERALES
  - SECCIÓN 2ª COORDINACIÓN EN EL MARCO DE LOS PROCEDIMIENTOS ESTABLECIDOS EN EL REGLAMENTO (UE) 2016/679

Título VIII. Procedimientos en caso de posible vulneración de la normativa de protección de datos

Título IX. Régimen sancionador

Título X. Garantía de los derechos digitales

Disposiciones adicionales

Disposiciones transitorias

Disposiciones finales

# NUEVO MODELO DE PRIVACIDAD

**De la gestión de los datos al gobierno responsable de la información.**

**Protección de datos más allá del territorio UE**

**Aproximación a la protección de datos basada en el riesgo**

**RESPONSABILIDAD PROACTIVA**(ART. 24)

**Privacidad desde el diseño** (art. 25)

**Privacidad por defecto** (art. 25)

**Registro de las actividades de tratamiento** (art. 30)

**Nuevo modelo de seguridad** (arts. 32-34)

# NUEVO MODELO DE PRIVACIDAD

**Evaluación de impacto a la protección de datos** (art. 35)

**Delegado de protección de datos** (arts. 37-39)

**Autorregulación y certificación** (arts. 40-43)

**Fortalecimiento de la posición de los titulares de los datos**

- **Consentimiento (arts. 4 y 6-8)**
- **Nuevos derechos (olvido –art. 17-, portabilidad –art. 20-)**
- **Derecho a indemnización (art. 82)**

**Fortalecimiento de las autoridades de protección de datos.**

**Modelo sancionador más severo**

## Responsabilidad
(art. 24)

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

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

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

**Privacidad desde el diseño**

(Art. 25.1)

El responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

**Privacidad por defecto**

(Art. 25.2)

El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

## PRINCIPIOS

Principios relativos al tratamiento (art. 5)

- **Licitud, lealtad, transparencia**
- Limitación de finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

Licitud del tratamiento (art. 6)

**Condiciones para el consentimiento (art. 7): definición: art. 4.11)**

Consentimiento del niño en relación con los servicios de la sociedad de la información (art. 8)

**Tratamientos de categorías especiales de datos (art. 9)**

Tratamiento de datos relativos a condenas e infracciones penales (art. 10): garantías adecuadas; control de las autoridades públicas.

## *Artículo 6 Licitud del tratamiento*

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger **intereses vitales** del interesado o de otra persona física;

**e) el tratamiento es necesario para el 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 intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Artículo 8.2 de la LOPDGDD:

El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

**LOPDGG: Artículo 28. Documentos aportados por los interesados al procedimiento administrativo.**

…….

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. **La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello.** No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

……

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, **salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso**. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.

## LOPDGDD:

**Disposición adicional octava.** ***Potestad de verificación de las Administraciones Públicas.***

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

**Disposición adicional décima.** ***Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.***

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

## LOPDGDD:

**Disposición adicional duodécima.** ***Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.***

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

***Artículo 9 Tratamiento de categorías especiales de datos personales***

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del **Derecho laboral y de la seguridad y protección social**, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger **intereses vitales** del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro,…..

e) el tratamiento se refiere a datos personales que el interesado ha hecho **manifiestamente públicos**;

h) el tratamiento es necesario para fines de **medicina preventiva o laboral**, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o **gestión de los sistemas y servicios de asistencia sanitaria y social**, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario **por razones de interés público** en el ámbito de la **salud pública**, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la **asistencia sanitaria** y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

## DERECHOS DEL INTERESADO

**Ejercicio manifiestamente infundado o excesivo (art. 12.5).**

**Transparencia (información). Art. 12, 13 y 14** (incluido información sobre plazo de conservación)

**Acceso (art. 15) (**incluidas las garantías en caso de transferencias; derecho a obtener una copia: art. 15.3)

**Rectificación** (art. 16)

**Supresión** (art. 17)

**Limitación del tratamiento** (art. 18)

**Obligación de notificación** (art. 19).

**Derecho a la portabilidad** (art. 20)

**Derecho de oposición** (art. 21)

**Decisiones individualizadas** (art. 22)

*Artículo 12 Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado*

*Artículo 13 Información que deberá facilitarse cuando los datos personales se obtengan del interesado*

*Artículo 14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado*

AEPD: Guía para el cumplimiento del deber de informar

Guidelines on transparency under Regulation 2016/679

WP 260

# LOPDGDD

**Artículo 11.** *Transparencia e información al afectado.*

1. Cuando los datos de carácter personal sean **obtenidos del afectado** el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La **información básica** a la que se refiere el apartado anterior deberá contener al menos:

a) La identidad del responsable del tratamiento o de su representante, en su caso.

b) La finalidad del tratamiento.

c) El modo en que el afectado podrá ejercitar los derechos establecidos en los **artículos 15 a 22 del Reglamento** (UE) 2016/679.

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 deberá 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 de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679 .

3. Cuando los datos de carácter personal **no hubieran sido obtenidos del afectado,** el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquél la información básica señalada en el apartado 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:

a) Las categorías de datos objeto de tratamiento.

b) Las fuentes de la que procedieran los datos.

# **Derecho a la portabilidad** (art. 20 RGPD)

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

a) el tratamiento esté basado en el consentimiento o en un contrato, y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

**ART. 29 WP: Guidelines on the right to data portability**
**(13-12-2016). WP 242**

**ART. 29 WP: Directrices sobre el derecho a la portabilidad de los datos**
**Adoptadas el 13 de diciembre de 2016 . Revisadas por última vez y adoptadas el 5 de abril de 2017**
**WP 242 rev.01**

## Derecho a la portabilidad

## LOPDGDD

**Artículo 17.** *Derecho a la portabilidad.*

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

## RGPD

(68) ……. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

Derivado de la disposición adicional decimocuarta LOPDGDD:

Las Administraciones tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, **denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22** del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

## RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO

**RGPD:**

Corresponsables del tratamiento (art. 26).

Encargado del tratamiento (art. 28)

- Contrato
- Subencargados

**LOPDGDD: Título V**

**Encargado del tratamiento (art. 33)**

**Ley 9/2017 (LCSP)**

**Disposición adicional vigésima quinta. Protección de datos de carácter personal.**

**RGPD: Artículo 28**

1.Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, **este elegirá únicamente** un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

**LOPDGDD: art. 33.5**

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.

**LOPDGDD: Disposición transitoria quinta. *Contratos de encargado del tratamiento.***

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

## REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

## RGPD:

Art. 30

- Del responsable
- Del encargado
- Por escrito
- A disposición de la Autoridad de Control
- No es obligatorio para ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales, o datos personales relativos a condenas e infracciones penales

## REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO
## LOPDGDD

Art. 31

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

**2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.**

## REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

### LOPDGDD

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«Artículo 6 bis. *Registro de actividades de tratamiento.*

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

## SEGURIDAD DE LOS DATOS

Art. 5. Principios.

1. Los datos personales serán:

f) tratados de tal manera que se garantice una **seguridad adecuada** de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

## *Artículo 32* **Seguridad del tratamiento**

1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

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.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los **riesgos** que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un **código de conducta** aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos **siguiendo instrucciones del responsable**, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

# NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

Art. 4. 12) «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;

Notificación de violaciones de seguridad a la autoridad de control (art. 33)

- En todo caso.
- Sin dilación:  a ser posible, antes de 72 horas
- El encargado debe notificar al responsable (art. 33.2)

Notificación de violaciones de seguridad al interesado (art. 34)

- Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas
- Excepciones (34.3)

**Guidelines on Personal data breach notification under Regulation 2016/679**
**Adopted on 3 October 2017**
**WP250**

**LOPDGDD: Disposición adicional primera. *Medidas de seguridad en el ámbito del sector público.***

1. 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 artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán 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.

# EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

Art. 35

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un **alto riesgo** para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

Asesoramiento del DPO

Supuestos en los que es obligatoria

Contenido mínimo

Valor de los códigos de conducta

**Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679**

**Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017**

**WP 248 rev.01**

# DELEGADO DE PROTECCIÓN DE DATOS

- Supuestos en los que es posible (u obligatorio) su nombramiento (art. 37).
- Régimen (art. 37)
- Posición (art. 38)
- Funciones (art. 39)

## Designación del DPO

## LOPDGDD

**Artículo 34**. *Designación de un delegado de protección de datos.*

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

……..

## DELEGADO DE PROTECCIÓN DE DATOS
## LOPDGDD: Arts. 34 a 37

**Art. 37:** ***Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.***

1. 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.

2. 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.

3. 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.

## TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAISES U ORGANIZACIONES INTERNACIONALES

(Arts. 44-50)

**Principio general**

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el mismo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional

# LOPDGDD

Artículos 40 a 43

Disposición adicional decimotercera. *Transferencias internacionales de datos tributarios.*

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

## AUTORIDADES DE CONTROL INDEPENDIENTES

(arts. 51-59)

**INDEPENDENCIA**

**COMPETENCIAS, FUNCIONES Y PODERES**

- Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.
- La autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como **autoridad de control principal** para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado

## COOPERACIÓN Y COHERENCIA

(Arts. 60-67)

## REGIMEN SANCIONADOR

Poderes correctivos de las autoridades de control (art. 58.2)

Multas:

- Circunstancias concurrentes (art. 83.2 y 3)
- Cuantía de las multas (art. 83.4, 5 y 6)
  - Hasta 10.000.000 € o, tratándose de empresas, hasta 2% volumen de negocio total anual global
  - Hasta 20.000.000 € o, tratándose de empresas, 4 % volumen de negocio total anual global
- **Posible multa a las AAPP (art. 83.7): decisión de cada Estado**

**Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679**

**3 de octubre de 2017**

**WP 253**

# REGIMEN SANCIONADOR
# LOPDGDD

**TÍTULO IX. Régimen sancionador**

Artículo 70. Sujetos responsables.

Artículo 71. Infracciones.

Artículo 72. Infracciones consideradas muy graves.

Artículo 73. Infracciones consideradas graves.

Artículo 74. Infracciones consideradas leves.

Artículo 75. Interrupción de la prescripción.

Artículo 76. Sanciones y medidas correctivas.

**Artículo 77. Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.**

Artículo 78. Prescripción de las sanciones.

## LOPDGDD: Disposición adicional tercera. *Cómputo de plazos.*

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

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá 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 entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

**Disposición adicional séptima.** ***Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.***

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su **nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad,** 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 mencionados en los dos párrafos anteriores, se identificará 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.

2. 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.

**Disposición final decimocuarta.** ***Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.***

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

«j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

# MUCHAS GRACIAS

jlpinarm@gmail.com
jlpinar@ceu.es