

El nuevo marco jurídico de la protección de datos personales. De dónde venimos y hacia dónde vamos. Principales novedades del **nuevo RGPD**.

Eduard Chaveli Donet
@eduardchaveli

Abogado. CEO en Gouvertis

1. ADMINISTRACIÓN ELECTRÓNICA, SEGURIDAD Y PROTECCIÓN DE DATOS

ANTES: Art. 42 de la Ley 11/2007 (Administración electrónica).

AHORA: La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo que deroga:

- a) Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- b) Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos

Y la Ley 40/2015, de Régimen Jurídico del Sector Público (LRJSP).

¡ La relación con estas y otras normas será desarrollada en la ponencia de Ana Marzo !

Se menciona la **seguridad y la protección de datos** como piezas fundamentales de la Administración Electrónica.

¿De qué sirve una administración que 365 x 24 si no podemos garantizar que sea segura en sus diferentes dimensiones y por tanto también la privacidad?

¿PORQUÉ HABLAMOS DE ENS SI EL TITULO ERA LA PROTECCIÓN DE DATOS?

Porque en el sector Público la protección de datos (antes LOPD, ahora RGPD) están relacionados.

Ya el RD 3/2010 que regulaba el ENS decía que cumplir el ENS presupone cumplir con la protección de datos, porque el ENS supone proteger la información y entre esa información obviamente se encuentran datos de carácter personal.

El ENS exige proteger la información relevante (contenga datos de carácter personal o no) que manejan tanto las AAPP, entes de naturaleza bifronte y empresas que prestan servicios a AAPP.



No podemos abordar los proyectos de RGPD sin tener en cuenta el ENS. Están relacionados

2. PONGAMOS EL FOCO EN LAS NOVEDADES DEL RGPD

2.1. NUEVO MARCO NORMATIVO

- ☐ **RGPD.** Deroga la Directiva 95/46/CE.
 - ☐ **Nueva LOPD.** Actualmente existe un proyecto **(PLOPD)**
 - ☐ **No se derogan ciertas disposiciones.**
- Ej. LSSI. Spam. Furturo Reglamento E-Privacy
- ☐ Existe en el **sector público** una conexión con el **ENS.**

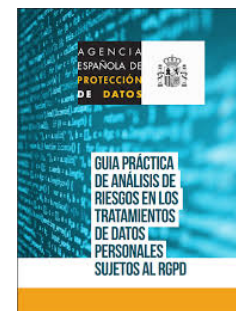


2.2. EL RGPD: OBJETIVO Y EXIGIBILIDAD

- ☐ Intento de **armonizar u homogeneizar** la normativa en privacidad a nivel europeo.
- ☐ Entró en vigor el 24 de mayo de 2016.
- ☐ Efecto directo. **No requiere trasposición al derecho interno.**
- ☐ **Será exigible a partir del 25 de mayo de 2018.**
- ☐ Hasta la fecha deberemos realizar una adaptación progresiva.
- ☐ Se va a aprobar una “nueva LOPD”. Existe un Proyecto.
- ☐ Reto de gran envergadura actual : **ADAPTARSE AL RGPD.**

2.3. DOCUMENTOS DE AYUDA AUTORIDADES DE CONTROL Y OTROS

¡¡ Existen materiales de ayuda. Se citan en la parte final !!



ARTICLE 29

Data Protection Working Party

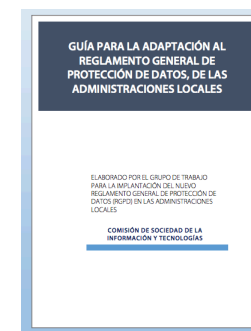


EL NUEVO RGPD Y SU IMPACTO SOBRE LA ACTIVIDAD DE LAS ADMINISTRACIONES LOCALES

Las Administraciones Públicas (AAP), y dentro de ellas las Administraciones Locales (AL), actúan como responsables y encargados de tratamiento de datos personales en el desarrollo de muchas de sus actividades. Consecuentemente, se ven afectadas por las prescripciones del nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea. En muchos casos, los efectos del RGPD sobre los mismos que para cualquier otro responsable o encargado. En algunos casos, sin embargo, existen especificidades.

El RGPD ha publicado en mayo de 2016 y entró en vigor en ese mismo mes. Sin embargo, se aplicó a partir del 25 de mayo de 2018. Las modificaciones que deberán realizarse para adecuar la actividad de las AL con las prescripciones del RGPD tendrán de carácter urgente, a más tardar, en esa fecha de 2018.

El impacto del RGPD sobre las AAP puede sintetizarse en los siguientes puntos:



2.4. PRINCIPALES NOVEDADES Y OBLIGACIONES

- ✓ Ampliación ámbito territorial de aplicación
- ✓ Viejos y nuevos conceptos
- ✓ Viejos y nuevos principios
- ✓ El tratamiento como protagonista
- ✓ El registro de las actividades de tratamiento
- ✓ Cambios en los derechos del titular de los datos
- ✓ Cambio en el enfoque de las medidas de seguridad
- ✓ Evaluaciones de impacto
- ✓ Cambios en las reglas de licitud del tratamiento.
- ✓ Cambios en el deber de información
- ✓ Nueva figura del delegado de protección de datos
- ✓ Diferente régimen sancionador
- ✓ Autoridades de control



Ampliación del ámbito territorial de aplicación

LOPD



- Responsables y encargados del tratamiento establecidos en la UE o no establecidos en la UE, cuando **utilicen para el tratamiento medios en territorio europeo**.

RGPD



- Responsables y encargados del tratamiento de datos personales **independientemente de su localización, cuando realicen tratamiento de datos de ciudadanos de la UE** para ofrecerles productos y servicios o realizar un seguimiento sobre ellos.

Nuevo enfoque: Responsabilidad proactiva

RGPD requiere que las organizaciones:

1. Analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de **operaciones de tratamiento** llevan a cabo.
2. **Determinen de forma explícita** la forma en que aplicarán las **medidas previstas en el RGPD**, asegurándose de que son las adecuadas y que lo pueden demostrar ante los interesados y las autoridades de supervisión.

RGPD exige una **actitud consciente, diligente y proactiva** por parte de las organizaciones frente a todos los tratamientos de datos.

En la práctica será importante conectar la “capa normativa” (registro de actividades) con las evidencias.

2.5. COMPARATIVA LOPD / RGPD.



Hay trabajo reutilizable



- Notificación e inscripción de ficheros al RGPD
- Deber de información
- Legitimación del tratamiento y reglas consentimiento.
- Contratos con encargados del tratamiento
- Documento de seguridad e implantación de medidas de seguridad de carácter técnico y organizativo en el sistema de información.
- Formación a Responsables y usuarios
- Derechos A.R.C.O.
- Auditoria bienal de las medidas de seguridad

- Registro de Actividades de Tratamiento + medidas
- Cambios en deber de información
- Cambios en legitimación, consentimiento y menores.
- Cambios en los contratos de encargo de tratamiento
- Responsabilidad proactiva:
 - Medidas documentadas pero no DS
 - Notificación violaciones de seguridad
 - Privacidad desde el diseño y por defecto
 - Evaluaciones de Impacto en la Privacidad (EIPD)
 - DPO
- Además de usuarios y responsables a DPO
- ARCO + Limitación + portabilidad y Derecho olvido
- Auditorias cuando determine el responsable

A. Registro de Actividades de Tratamiento de datos personales [Artículo 30 RGPD]



Nombre del **AGENDA CONTACTOS TERCEROS**

fichero:

Finalidad: CONTIENE DATOS DE CONTACTO DE TERCEROS EN GENERAL NECESARIOS PARA EL MANTIEMIENTO DE LA RELACION CON LOS MISMOS

Nombre del **CONTABILIDAD**

fichero:

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

Nombre del **CURRICULUMS**

fichero:

Finalidad: GESTION DE SELECCION Y PROMOCION DE PERSONAL

Nombre del **EXPEDIENTES**

fichero:

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

Nombre del **PROVEEDORES**

fichero:

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

☐ **NO notificación a la autoridad de control.**

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

☐ En la práctica = Información NOTA + otra + Descripción general de medidas

• Recomendación ¿Cómo articular el Registro de Actividades de Tratamiento?



[Vid. *Guía del RGPD para Responsables de Tratamiento*]



1º Partir de los ficheros que actualmente tienen inscritos

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



Pongamos el foco en los tratamientos. Si granulamos demasiado no podremos ni despegar ni mantener el proyecto

EJEMPLO DEL ESTRUCTURA DEL REGISTRO DE ACTIVIDADES

1. NOMBRE DEL TRATAMIENTO
2. CONJUNTO DE DATOS AL QUE ESTÁ VINCULADO (FICHERO)
3. DATOS DE CONTACTO.
4. FINALIDAD DEL TRATAMIENTO Y CAUSA DE LICITUD
5. CATEGORÍAS DE INTERESADOS
(Hasta ahora en el NOTA ORIGEN Y PROCEDENCIA DE LOS DATOS)
6. CATEGORÍAS DE DATOS PERSONALES
 - 6.1. TRATAMIENTO DE DATOS PERSONALES QUE NO CONSTITUYAN CATEGORÍAS ESPECIALES
 - 6.2. TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS PERSONALES
 - 6.3. DATOS DE CONDENAS Y DELITOS
7. CATEGORÍAS DE DESTINATARIOS A QUIENES SE HAN COMUNICADO O VAN A COMUNICARSE LOS DATOS PERSONALES (en particular los destinatarios de terceros países, cuando no sean TID)
 - 7.1. CESIONES
 - 7.2. ENCARGADOS DEL TRATAMIENTO
8. CATEGORÍAS DE TRANSFERENCIAS DE DATOS PERSONALES A UN TERCER PAÍS [TID] O A UNA ORGANIZACIÓN INTERNACIONAL
9. LOS PLAZOS PREVISTOS PARA LA SUPRESIÓN DE LAS DIFERENTES CATEGORÍAS DE DATOS (CUANDO SEA POSIBLE) SEGÚN CADA FINALIDAD
10. UNA DESCRIPCIÓN GENERAL DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD (CUANDO SEA POSIBLE)
Sólo un listado a modo de índice o descripción general con remisión a los concretos procedimientos.



EJEMPLOS DE TRATAMIENTOS

FICHEROS	ACTIVIDADES DE TRATAMIENTO
1. BIBLIOTECA MUNICIPAL	<ol style="list-style-type: none"> 1. Gestión de Prestamos de obras audiovisuales 2. Gestión sobre la confección de carnés de socios.
2. PROVEEDORES	<ol style="list-style-type: none"> 1. Gestión de proveedores (se comprenderá la gestión de proveedores, administrativa – contratación o pedidos - económica o contable, fiscal, pagos de obras, bienes o servicios)
3. RECURSOS HUMANOS; TRABAJADORES; PERSONAL; EMPLEADOS	<ol style="list-style-type: none"> 1. Gestión de Recursos Humanos (contratación, altas, bajas, permisos, promoción...) 2. Gestión de nóminas 3. Prevención de riesgos laborales 4. Formación del personal 5. Selección de personal (oposiciones y concursos y promoción y selección de personal) 6. Prestación de servicios de certificación electrónica <p><u>OTROS</u></p> <ol style="list-style-type: none"> 1. Control horario o de presencia en el puesto de trabajo (tarjeta magnética, biométrica) 2. Revisión y/o asistencia médica de la propia organización 3. Acción Social a favor del personal de la organización
Etc.	



Y DICE EL #PLOPD QUE HAY QUE PUBLICARLO

Artículo 33. Registro de las actividades de tratamiento.

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. Las Administraciones Públicas 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.



**¿Cuál es el problema que
ello puede producir?**

B. Deber de información [Artículo 13 y 14 RGPD] (Cláusulas)

☐ Además de la información establecida por la LOPD, se han de añadir otros extremos:

- Datos de contacto del **Delegado de Protección de Datos**.
- **La base jurídica o legitimación para el tratamiento**
- Informar de las **transferencias internacionales de datos**.
- **Plazo s o criterios de conservación de los datos**.
- **La previsión de transferencias a Terceros Países**.
- **Derecho reclamación** ante una autoridad de control.

☐ Y, en el caso de que los datos no se obtengan del propio interesado:

- El **origen** o procedencia de los datos
- Las **categorías o tipos de datos** (identificativos, características personales, etc.)



#PLOPD

Información por capas

☐ Primera capa. Información básica

☐ Supuestos:

1. Datos recabados del afectado en redes de comunicaciones electrónicas o servicios de la sociedad de la información
2. Lo disponga la Ley
3. O lo autorice la AEPD

☐ Información básica

1. Identidad del responsable
2. Finalidad del tratamiento
3. Forma de ejercer los derechos
4. Y dirección electrónica para acceder a la **segunda capa de información**



DIFERENTES ENTORNOS O VÍAS

Información básica (1ª capa)	Información adicional (2ª capa)
Dónde ha de recogerse	
Debería situarse en el mismo "campo de visión" , según sea el medio utilizado en la recogida de los datos	Depende de las características del medio empleado para informar, si bien ya no debe estar condicionada en cuanto a la extensión de la información. Las posibilidades, en este caso, son más flexibles.
En papel	
Debería situarse en el mismo lugar donde están los campos a cumplimentar. Si, por restricciones del diseño, no fuese factible, debe incorporarse una nota o llamada en el campo de visión de la firma, informando sobre dónde se sitúa la tabla con la información sobre protección de datos. Ejemplo: <i>"antes de firmar la solicitud, debe leer la información básica sobre protección de datos que se presenta en (...el reverso, al pie, etc...)"</i>	<ul style="list-style-type: none"> • En el mismo formulario cumplimentado (por ejemplo, en el reverso) • Como un anexo o separado que se entregue al interesado y que pueda conservar • Como información expuesta, claramente visible, en carteles, paneles, trípticos, etc., de los cuales se pueda solicitar una copia manejable para conservar.
Medios electrónicos	
Debería situarse donde está el botón de "Enviar" . Es recomendable que, para información adicional o complementaria, se incluya en hipervínculo a la misma. Ejemplo: + info .	<ul style="list-style-type: none"> • En una página web específica, a la que se accede mediante un hipervínculo • Como un documento disponible para su descarga desde una URL • Como información anexa o adjunta a un mensaje electrónico dirigido al interesado
Telefónicamente	
Como una locución clara y concisa, pero asegurando que el interlocutor haya comprendido la información suministrada, antes de proceder a la recogida de la información. Se ofertará poner a su disposición la información adicional por otro medio, pero si el interesado solicita alguna aclaración se le deberá ofertar una locución complementaria con la información adicional correspondiente al epígrafe sobre el que se haya interesado.	Como una locución que se le ofrezca al interesado, como complemento o alternativa a una oferta de disponibilidad de información adicional accesible electrónicamente o remitida, por correo postal o electrónico.



Información mediante iconos estandarizados

- ❑ La importancia que el RGPD concede a la **claridad y accesibilidad** de la información se refleja previsión de información por iconos.
- ❑ El diseño de estos iconos deberá hacerlo la **Comisión Europea**, que ya **está trabajando para presentar una propuesta**.

INFORMACIÓN ESENCIAL		CUMPLIMIENTO
	No se recaban datos más allá de los necesarios para cada tratamiento concreto	
	No se conservan datos más allá de los necesarios cada tratamiento concreto	
	No se tratan datos con finalidades distintas a la principal	
	No se ceden datos a terceros para finalidades distintas a la que principal	
	No se venden	
	No se conservan datos sin cifrar	

C. Licitud o legitimación en el tratamiento

- El consentimiento deja de ser la RG para ser “una causa mas”:
 - Ejecución de un contrato (hacer referencia a contrato o tipo de contrato)
 - **Cumplimiento del deber de una obligación legal** (indicar la norma con rango de Ley. **Art.8.2. PLOPD**)
 - **Misión en interés público o ejercicio de poderes públicos** (indicar la norma con rango de Ley. **Art. 8.2. PLOPD**)
 - ~~Interés legítimo de responsable o tercero~~ (explicitar el interés y buena práctica ponderación)
(“...no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones”)
 - Excepcionalmente en supuestos de urgencias: Protección de intereses vitales
 - Consentimiento del interesado
 - Debe de ser “inequívoco” y “explícito”. No tácito.
 - Lenguaje claro y sencillo
 - Revocable
 - Carga de la prueba el responsable

D. Regularización de los prestadores de servicios con acceso a datos (= Encargados de Tratamiento)

¿Quién es el Encargado de Tratamiento? = Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

EJEMPLOS DE ENCARGADOS

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

- ☐ Contrato o acto jurídico similar que los vincule.
 - ☐ Deberá constar **por escrito**, inclusive en formato electrónico.
 - ☐ **AEPD: NOVEDAD:** *"La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una novedad del RGPD".*
- ☐ Pero matiza que "en cualquier caso debe tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre y cuando ese acto vincule jurídicamente al encargado del tratamiento.

UN EJEMPLO: resolución administrativa que conste notificada al encargado del tratamiento.



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

Los *contratos de encargo concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar este contenido, sin que sean válidas* las remisiones genéricas al artículo del RGPD que los regula.

1. Objeto, duración y naturaleza
 2. Finalidad del tratamiento/s que se autoriza al encargado
 3. Tipo de datos personales y categorías de interesados
 4. Que el encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable.
 5. Deber de confidencialidad, secreto profesional
- Dicho contrato o acto jurídico garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
 - El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable del tratamiento.

6. Medidas de seguridad, técnicas y organizativas.

- Realizar una Evaluación de impacto.
- A partir de aquí, la determinación de las medidas de seguridad concretas puede realizarse a través de una lista exhaustiva de las mismas o de la remisión a un estándar o marco nacional o internacional reconocido.

7. Régimen de subcontratación (condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones)

- La autorización puede ser específica (identificación de la entidad) o general (sólo autorizando la subcontratación, pero sin concretar entidad).
- Cuando sea general, el encargado informará al responsable de la incorporación de un subencargado o su sustitución por otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
- Puede ser de utilidad establecer en el acuerdo o acto la forma (que en todo caso deberá constar por escrito) y el plazo para que el responsable pueda manifestar su oposición.
- El subencargado del tratamiento debe estar sujeto a las mismas condiciones) y en la misma forma que el encargado del tratamiento.
- En caso de incumplimiento por el subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento

8. Colaboración en el cumplimiento de obligaciones del Responsable

Esta colaboración se refiere a los siguientes aspectos:

- Comunicación de violaciones de datos.
- Atención derechos de los interesados.
- Poner a disposición del Responsable la información necesaria para demostrar el cumplimiento de las obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, realizadas por el responsable o por otro auditor autorizado por el responsable.

9. Finalización de la relación: supresión o devolución de datos

10. Diligencia en la elección y supervisión del Encargado

- ☐ El Responsable de Tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes.
- ☐ Para demostrarlo el RGPD prevé que la adhesión a **CÓDIGOS DE CONDUCTA** o la posesión de un **CERTIFICADO** de protección de datos pueden servir como mecanismos de prueba.

Declaración de conformidad/certificación de conformidad

Sistemas de Categoría BÁSICA	• Es suficiente una DECLARACIÓN DE CONFORMIDAD que puede realizar la propia organización (o un tercero)
Sistemas de Categoría MEDIA	• La auditoría de CERTIFICACIÓN para los sistemas de categoría MEDIA Y ALTA es obligatoria.
Sistemas de Categoría ALTA	• Sólo pueden realizarlas ENTIDADES DE CERTIFICACIÓN ACREDITADAS POR ENAC

Logotipo de la Entidad Certificadora con marca de certificación acreditada

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

"<<Entidad Certificadora>>" certifica que los sistemas de información reseñados, todos ellos de categoría <<señalar categoría máxima aplicable (BÁSICA, MEDIA o ALTA)>> y los servicios que se relacionan, de << Entidad [pública o privada], dirección postal>>.

han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración, según se indica en el correspondiente Informe de Auditoría de <<fecha>> para:

<<enumerar los sistemas de información y los servicios objeto de la certificación>>.

Fecha de certificación de conformidad inicial: <<día>> de <<mes>> de <<año>>.
 Fecha de renovación de la certificación de conformidad: <<día>> de <<mes>> de <<año>>.

Número de certificado: <<número de certificado>>.

Fecha<<Localidad [la que corresponda]>>, <<día>> de <<mes>> de <<año>>.
 Firma: <<Nombre y Apellidos del responsable competente de la Entidad Certificadora>>.
 Firma del responsable de la Entidad Certificadora:

Nombre completo /razón social de la Entidad Certificadora y pág. web.
 Dirección postal/ electrónica.
 Código Postal, Provincia, País.

Nombre	Razón social	Enlace web	Estado Acreditación ENS
AENOR Internacional S.A.U.	AENOR Internacional S.A.U.	www.aenor.com	ACREDITADA (21/04/2017)
Audertis Audit Services, S.L.	Audertis Audit Services, S.L.	www.audertis.es	ACREDITADA (29/12/2017)

<https://www.ccn-cert.cni.es/ens/entidades-de-certificacion.html>

¿Moratoria en el PLOPD?

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 transcurridos cuatro años desde la citada fecha.

En caso de que los contratos previesen su prórroga al término de su vencimiento, ya fuera por mutuo acuerdo entre las partes o en ausencia de denuncia por cualquiera de ellas, deberá producirse su adaptación con anterioridad al momento en que estuviera prevista dicha prórroga.

E. Derechos del interesado

Al catálogo «tradicional» de derechos ARCO añade nuevos:

E.1.Portabilidad de los datos



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



Art.20.3 RGPD: 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.

E.2. Limitación



- ☐ Se trata del **marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro**
- ☐ **Supuestos:**
 - Cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
 - Cuando 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.
 - Cuando 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.
 - Cuando el interesado se haya opuesto al tratamiento ejercitando su derecho de oposición, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

E.3. Derecho al Olvido (supresión)



- ☐ **No** está considerado un **derecho autónomo o diferenciado** de los derechos ARCO, sino es la consecuencia de la aplicación del derecho al borrado. Es una **manifestación de los derechos de cancelación u oposición en el entorno on-line**.
- ☐ **Derecho** del ciudadano a **solicitar**, y obtener de los responsables, sin demora injustificada, **que sus datos personales sean suprimidos en el ámbito de Internet**:
 - ✓ Derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales.
 - ✓ El responsable del tratamiento, atendiendo a la tecnología disponible y el coste de su aplicación adoptará medidas razonables , incluso medidas técnicas, con el objeto de informar a los responsables correspondientes (supresión de enlaces, copia o réplica).
- ☐ Se prevén límites a su ejercicio.

Disposiciones generales derechos A.R.C.O.P.L

- ☐ **Gratuidad:** no obstante, se establecen los supuestos en los que el Responsable puede cobrar una tasa o canon razonable o incluso negarse a responder. Ej. solicitudes abusivas que manifiestamente infundadas, excesivas, o aquellas que tengan un carácter repetitivo.
- ☐ **Plazos:** se establece un plazo de **1 MES para hacer efectivo el derecho del interesado**, el cual puede ser prorrogado por 2 meses más en supuestos de complejidad o número de solicitudes recibidas.
- ☐ **Medios Electrónicos:** Se debe proporcionar medios para que las solicitudes se presenten por medios electrónicos.
- ☐ **Negativa a la solicitud:** en los supuestos en los que no se le conceda el ejercicio de derechos deberá ser informado en el mismo **plazo de un mes de los motivos y la posibilidad** de presentar la correspondiente **reclamación ante la Autoridad** competente.
- ☐ **Información adicional:** en aquellos casos en los que existan dudas razonables sobre la identidad de la persona física que realiza la solicitud.

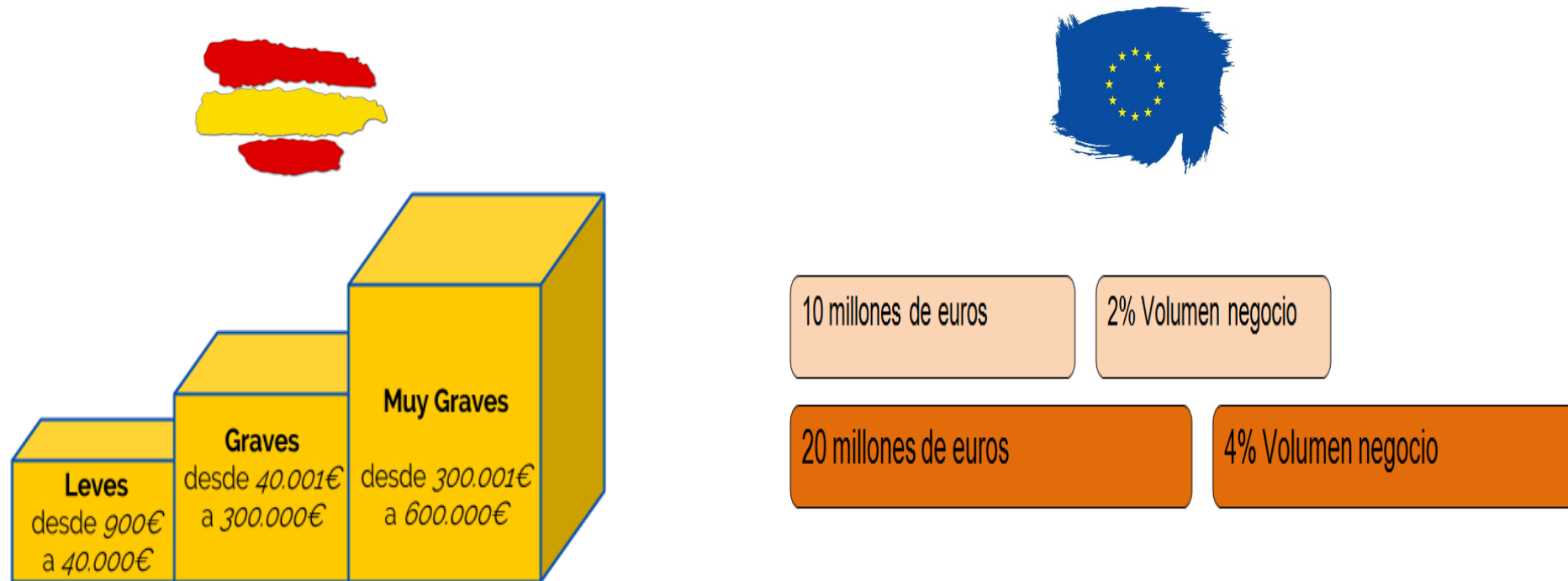
F. Seguridad

¡ Estos aspectos serán desarrollados en la siguiente ponencia por Javier Cao !

- ☐ Cambios en la determinación de las medidas: Análisis de riesgos
- ☐ Relación con el ENS
- ☐ Notificación de las violaciones, quiebras o brechas de seguridad
- ☐ Privacy by design
- ☐ Privacy by default
- ☐ Auditorías (periodicidad no definida directamente)



G. ENDURECIMIENTO DE LAS SANCIONES



#PLOPD No contempla sanciones económicas para el sector público

❑ **No habrá sanciones económicas** a AAPP a pesar de que el RGPD lo permite. No las prevé el **PLOPD**

❑ **Si otras.** Cada autoridad de control dispondrá de todos los siguientes poderes correctivos:

- Sancionar a todo responsable o encargado del tratamiento con una **advertencia** cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;
- Sancionar a todo responsable o encargado del tratamiento con **apercibimiento** cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
- **Retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida** con arreglo a los artículos 42 y 43, **u ordenar al organismo de certificación que no se emita una certificación** si no se cumplen o dejan de cumplirse los requisitos para la certificación;
- **Ordenar la suspensión de los flujos de datos hacia** un destinatario situado en un **tercer país** o hacia una organización internacional.
- Posibilidad de **obligar a realizar auditorías periódicas**.

¡ Sin perjuicio del derecho a indemnización mediante procedimiento de responsabilidad patrimonial !

H. Deberemos nombrar un DPD o DPO

¡ Estos aspectos serán desarrollados en la sesión de tarde por Eusebio Moya !

¡¡ Yo de mayor quiero ser DPD !!



I. HAY QUE TENER UNA HOJA DE RUTA DEL RGPD

“No hay viento favorable para el que no sabe dónde va”

Séneca





¡ El 25 de mayo es un hito pero la seguridad y la protección de datos es un proceso de mejora continua !



¡ Y debemos de saber PRIORIZAR hitos y adaptarnos a los problemas del camino !



3. PARA QUIENES QUIERAN PROFUNDIZAR

<https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php>

<https://dpd.aec.es/blog/>

<http://www.govertis.com/formacion/blog>



Inicio Servicios Historia Productos G.R.C. Clientes Acceso Plataformas Blog Trabaja con Nosotros

Blog

REGISTRO DE ACTIVIDADES II

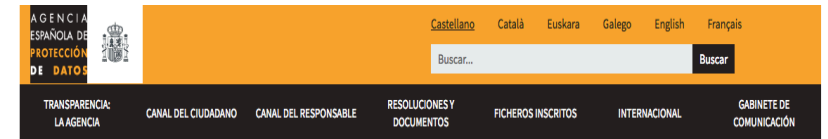
Posted on 11 enero, 2018 by govertis

CÓMO ELABORAR EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO II Eduard Chavell Donet. IT Lawyer and CEO at GOVERTIS @eduardchavell 2. ¿QUIÉN TIENE QUE LLEVAR EL REGISTRO DE ACTIVIDADES? El Registro de Actividades de Tratamiento lo deberán llevar a cabo cada responsable y encargados y, en su caso, sus representantes. Pero el[...]

Posted in Blog Leave a comment

CATEGORÍAS

- Blog (31)
- Formación (2)
- Noticias (15)
- Ofertas de Empleo (2)
- Recursos (4)



Temas ▶ Reglamento ▶ index ▼

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD), que sustituirá a la actual normativa vigente y que comenzará a aplicarse el 25 de mayo de 2018. Este periodo de dos años tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones y también las empresas y organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

Esta sección, que se actualizará progresivamente, agrupa las diferentes iniciativas que la Agencia Española de Protección de Datos ha puesto en marcha sobre el RGPD, de forma que ciudadanos y organizaciones puedan localizar con mayor facilidad materiales de utilidad en relación a la nueva normativa.

915 752 750 aec@aec.es



HOME PROGRAMA AVANZADO DPO/DPO PROGRAMA SUPERIOR DPO/DPO BLOG DPO AEC

Delegado De Protección De Datos » Blog DPO



Entradas recientes

- La Protección De Datos En El Panorama Internacional. Una Primera Aproximación
- Los 10 Puntos Clave Del RGPD
- Quién Debe Ser DPO (DPO)
- Los Principios Generales De La Protección De Datos ¿Fundamentos Y/O Deberes?

¡¡ GRACIAS POR VUESTRA ATENCION !!

www.govertis.com

[@govertis](https://twitter.com/govertis)

info@govertis.com