



Reglamento Europeo de Protección de datos

M^a Belén Pose Vidal

Abogada.

Directora Asesoría Jurídica Corporativa ARAG





una nueva regulación ?



Rápida evolución tecnológica

Violaciones de seguridad



Generación masiva de datos

El dato personal

ARAG



Bases de licitud del tratamiento:



- consentimiento
- ejecución de un contrato
- cumplimiento de obligación legal
- interés vital
- interés público/poderes públicos
- interés legítimo

¿Cuáles son las principales diferencias ?



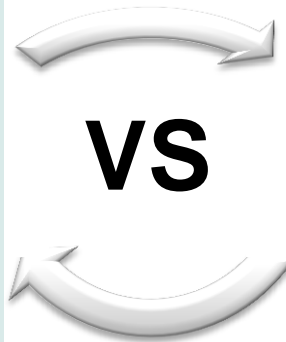
1. Ámbito de aplicación



LOPD 15/1999



- Responsable y tratamiento en territorio español
- Responsable no establecido en España, pero es aplicable la legislación española según normas de Derecho Internacional público.
- Responsable fuera UE pero utiliza en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.



RGPD



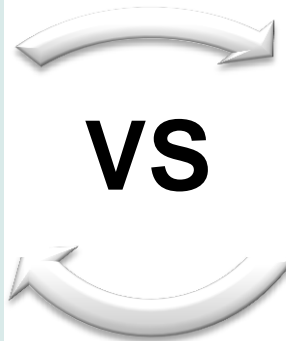
- Tratamiento de datos de residentes en la UE, aunque la empresa esté fuera de la UE, siempre que estén relacionados con la oferta de bienes o servicios a los **ciudadanos europeos**, o hagan un seguimiento de su conducta
- Tratamiento de datos personales por parte de **empresas establecidas en la UE**, independientemente de dónde lleven a cabo ese tratamiento.

2. Datos especialmente protegidos



LOPD 15/1999

- Salud
- Ideología
- Afiliación sindical
- Religión y creencias
- Origen racial
- Vida sexual
- Comisión de infracciones penales y administrativas



RGPD

- Salud
- Opiniones políticas
- Afiliación sindical
- Convicciones religiosas o filosóficas
- Origen étnico o racial
- Vida y orientación sexual
- Condenas e infracciones penales
- Datos genéticos
- Datos biométricos

3. Ficheros y tratamientos



LOPD 15/1999

- Inscripción obligatoria de los ficheros en el Registro General de Protección de Datos

VS

RGPD

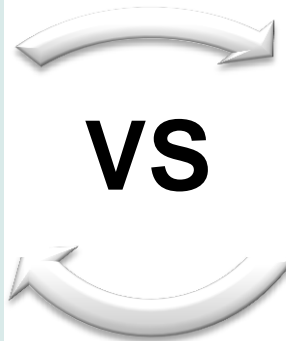
- Obligación de elaborar un registro de actividades de tratamiento teniendo en cuenta su finalidad y su base jurídica

4. Brechas de seguridad



LOPD 15/1999

- No hay obligación de comunicar brechas de seguridad



RGPD

- Obligación de notificar brechas de seguridad a la AEPD y en determinados casos, a los interesados.



5. Información



LOPD 15/1999

- Existencia de un fichero o tratamiento de datos, finalidad de su recogida y destinatarios de la información.
- Si es obligatorio o no contestar las preguntas
- Consecuencias de la obtención de los datos o de la negativa a facilitarlos
- Posibilidad de ejercitar derechos ARCO.
- Identidad y dirección de responsable del tratamiento.



GDPR

- Datos del contacto del DPO
- Base jurídica o legitimación para poder tratar los datos
- Plazo o criterios de conservación
- Existencia de decisiones automatizadas o elaboración de perfiles
- Previsión de transferencias fuera de la UE
- Derecho a reclamar ante la AEPD
- Origen y categorías de datos si no se han obtenido del propio interesado

¿Cómo habrá que facilitar la información?



Recomendaciones
AEPD para cumplir
con los requisitos de
información a partir
del 25 de mayo



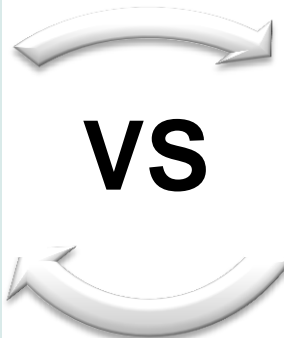
Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
“Responsable” (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
“Finalidad” (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
“Legitimación” (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
“Destinatarios” (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
“Derechos” (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
“Procedencia” (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

6. Consentimiento



LOPD 15/1999

- Se admite el consentimiento **tácito** o por omisión como una de las categorías del consentimiento **inequívoco**
- Se requiere consentimiento **expreso** y por escrito para datos sensibles



RGPD

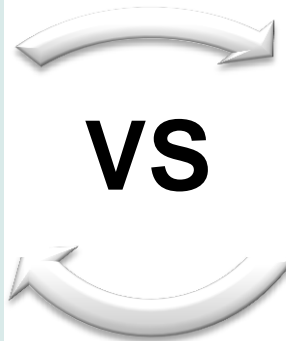
- El consentimiento debe ser siempre **inequívoco**, requiere de una manifestación del interesado o de una clara acción afirmativa.
- Se requiere consentimiento **explícito** para:
 - Datos sensibles
 - Decisiones automatizadas
 - Transferencias internacionales

7. Menores y servicios de la sociedad de la información



LOPD 15/1999

- No pueden prestar consentimiento (solos) los menores de 14 años



RGPD

- No pueden prestar consentimiento (solos) los menores de 16 años. Se permite a los Estados miembros establecer edad inferior . Tope 13 años.
- Proyecto de nueva LOPD: Se rebaja a 13 años.

8. Derechos



LOPD 15/1999

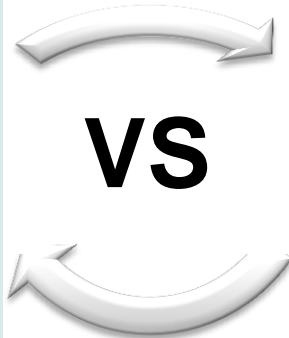
Acceso



Rectificación

Cancelación)

Oposición



RGPD

Acceso

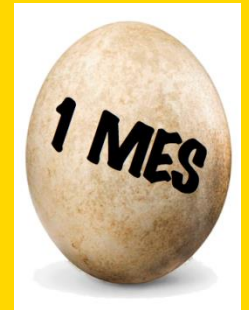
Rectificación

Supresión (Incluye el derecho al **Olvido**)

Oposición

Limitación del tratamiento

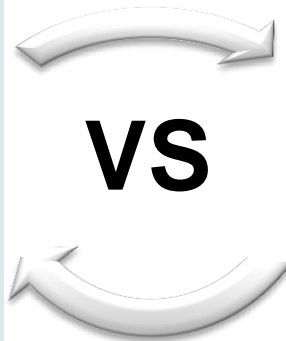
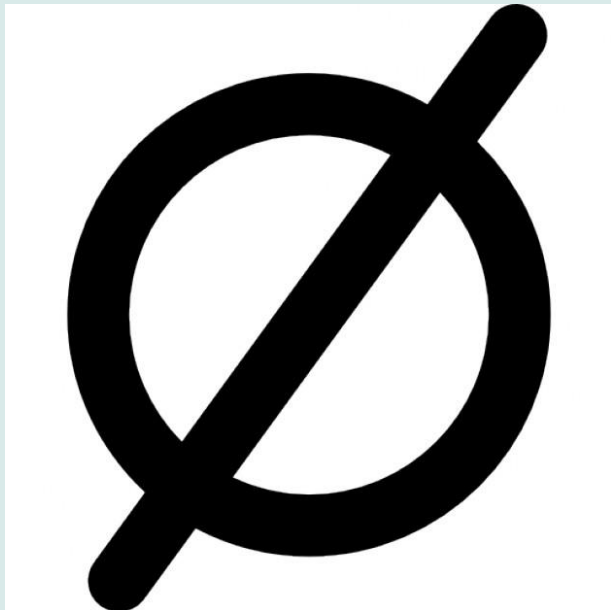
Portabilidad



9. Análisis de riesgo



LOPD 15/1999



RGPD

Todo tratamiento requiere un análisis de riesgo y en función del resultado, determinación de:

Medidas de seguridad

+

Medidas de protección
“desde el diseño”

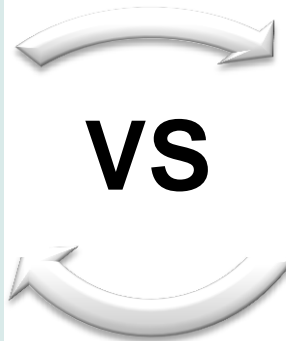
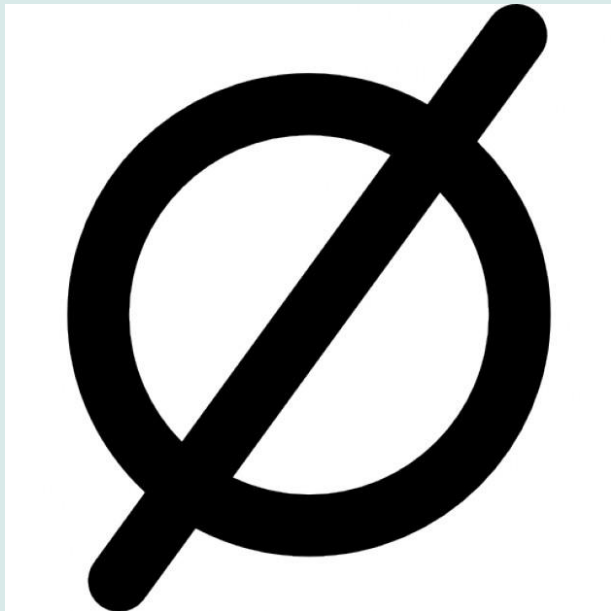
+

Necesidad de evaluaciones de
impacto (PIA)

10. Evaluación de impacto (PIAS)



LOPD 15/1999



RGPD

Cuando sea probable que un tratamiento, especialmente si se utilizan nuevas tecnologías, suponga un riesgo alto para los derechos y libertades de las personas, se tiene que hacer la evaluación de impacto y, en su caso, consultar a la AEPD **antes** del tratamiento.

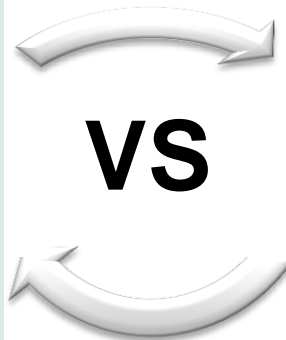
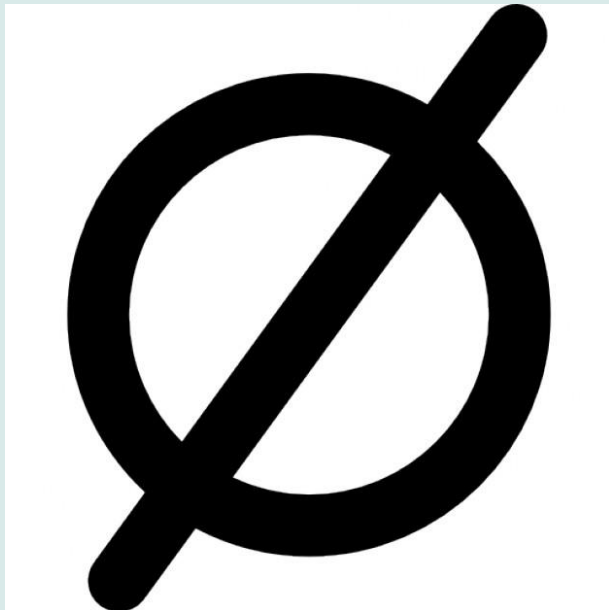
Ejemplos:

- Elaboración de perfiles para toma de decisiones con efectos jurídicos
- Tratamiento a gran escala de datos sensibles
- Observación sistemática a gran escala de zonas de acceso público.

11. Privacidad por defecto



LOPD 15/1999



RGPD

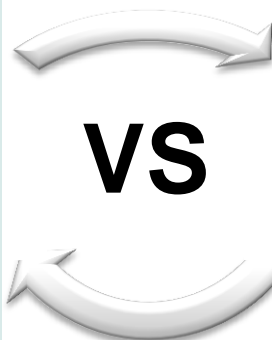
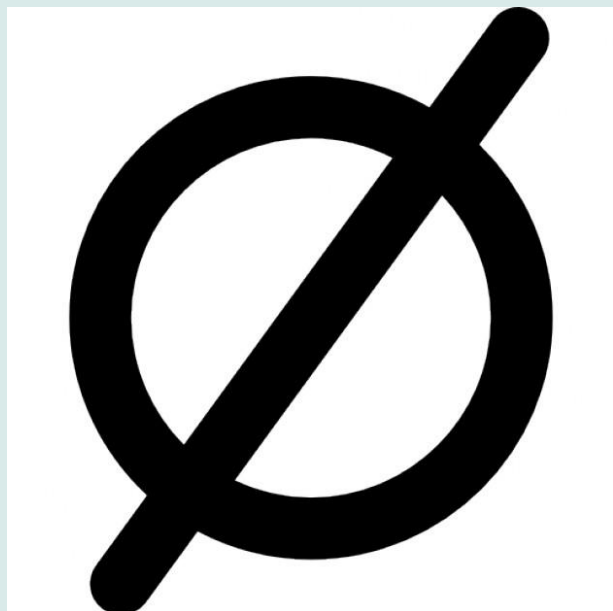
El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas para:

Garantizar que, por defecto, **sólo** se traten los **datos personales necesarios** para cada finalidad específica del tratamiento

12. Privacidad desde el diseño



LOPD 15/1999



RGPD

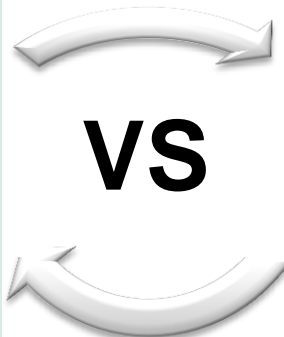
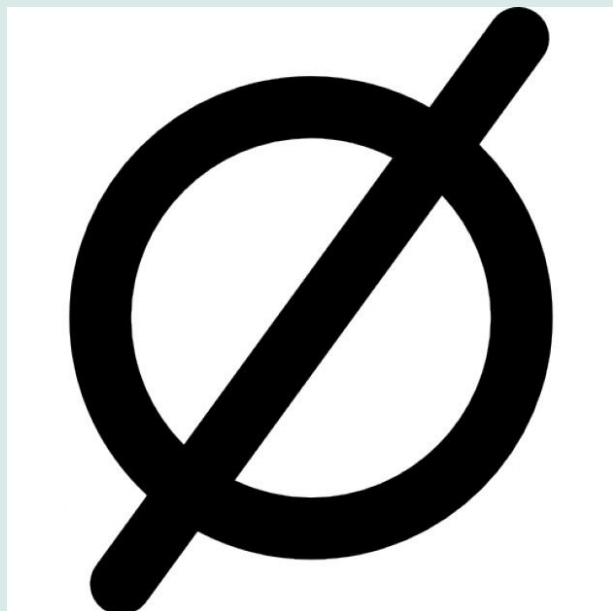
El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas para:

Proteger los datos y cumplir con las exigencias del Reglamento tanto en el momento de determinar los medios de tratamiento como en el momento del tratamiento mismo

13. Delegado de protección de datos



LOPD 15/1999



RGPD

DPD obligatorio para responsables y encargados de tratamiento:

- Autoridades y organismos públicos
- Empresas que traten a gran escala “datos sensibles”
- Empresas que hagan tratamientos que requieran una observación habitual y sistemática de interesados a gran escala.

! El Proyecto de LOPD establece una lista de actividades que estarán obligadas a disponer en todo caso de DPD

14. Sanciones



LOPD 15/1999

RGPD

VS

**Entre 900 €
y 600.000 €**

**Hasta
20.000.000€
ó el 4% de
facturación**

11 Claves para adaptarse

1

- Concienciación: Privacidad desde el diseño y por defecto. Responsabilidad proactiva.

2

- Revisar y completar las cláusulas informativas

3

- Obtener consentimiento explícito de los interesados

4

- Conocer y facilitar el ejercicio de los derechos

5

- Saber qué datos se tratan y con qué base legal

6

- 72 horas para comunicar violaciones de seguridad

7

- Corredor= responsable. Agente=encargado

8

- Control de los colaboradores externos. Adaptación de contratos.

9

- Registro de actividades de tratamiento

10

- ¿Necesito nombrar un Delegado de Protección de Datos?

11

- ¿Tengo que hacer evaluaciones de impacto (PIAS)?



BOLETÍN OFICIAL
DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

XII LEGISLATURA

Serie A:
PROYECTOS DE LEY

21 de mayo de 2018

Núm. 22-1

Pág. 1



Artículo 77. Condición de responsable o encargado del tratamiento.

1. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre:

a) Los agentes de seguros y los operadores de banca-seguros tendrán la condición de encargados del tratamiento de la entidad aseguradora con la que hubieran celebrado el correspondiente contrato de agencia, en los términos previstos en esta ley.

b) Los corredores de seguros y los corredores de reaseguros tendrán la condición de responsables del tratamiento respecto de los datos de las personas que acudan a ellos.

c) Los colaboradores externos a los que se refiere el artículo 11 tendrán la condición de encargados del tratamiento de los agentes o corredores de seguros con los que hubieran celebrado el correspondiente contrato mercantil. En este caso, sólo podrán tratar los datos para los fines previstos en el artículo 11.1.

2. En el supuesto previsto en la letra a) del apartado 1, en el contrato de agencia deberán hacerse constar los extremos previstos en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, y, en particular, la indicación de si el agente de seguros va a celebrar contratos mercantiles con los colaboradores externos a los que se refiere el artículo 11.

Del mismo modo, en el supuesto previsto en el apartado 1.d) deberán incluirse en el contrato mercantil celebrado con los colaboradores externos los extremos previstos en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre.



BOLETÍN OFICIAL DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

XII LEGISLATURA

Serie A:
PROYECTOS DE LEY

21 de mayo de 2018

Núm. 22-1

Pág. 1



Artículo 78. Otras normas de protección de datos.

1. En la publicidad que remitan a terceros los mediadores de seguros y reaseguros, a través de comunicaciones electrónicas, deberá estarse a lo dispuesto en los artículos 21 y 22.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

2. Los agentes de seguros y operadores de banca-seguros únicamente podrán tratar los datos de los interesados en los términos y con el alcance que se desprenda del contrato de agencia de seguros y siempre en nombre y por cuenta de la entidad aseguradora con la que hubieran celebrado el contrato.

Los operadores de banca-seguros no podrán tratar los datos relacionados con su actividad mediadora para fines propios de su objeto social sin contar con el consentimiento inequívoco y específico de los afectados.

3. Los corredores de seguros podrán tratar los datos de las personas que se dirijan a ellos, sin necesidad de contar con su consentimiento:

a) Antes de que aquéllos celebren el contrato de seguro, con las finalidades de ofrecerles el asesoramiento basado en un análisis objetivo y personalizado al que se refiere esta ley y de facilitar dichos datos a la entidad aseguradora con la que fuese a celebrarse el correspondiente contrato.

b) Después de celebrado el contrato de seguro, exclusivamente para ofrecerles el asesoramiento basado en un análisis objetivo y personalizado al que hace referencia la ley.

Para la utilización y tratamiento de los datos para cualquier otra finalidad distinta de las establecidas en las dos letras anteriores, los corredores de seguros deberán contar con el consentimiento de los interesados.

El corredor deberá facilitar a la entidad aseguradora para la firma del contrato de seguro los datos que a tal fin le hubieran sido facilitados por el cliente, sin modificarlos ni reemplazarlos por otros.

4. Resuelto el contrato de seguro en cuya distribución hubiera intervenido un corredor de seguros o un corredor de reaseguros, éste deberá proceder a la cancelación de los datos, a menos que el interesado le hubiera autorizado el tratamiento de sus datos para otras finalidades y, en particular, para la celebración de un nuevo contrato.

En todo caso, el corredor de seguros y el corredor de reaseguros no podrán facilitar los datos del interesado a otra entidad distinta de aquella con la que el interesado hubiera celebrado el contrato resuelto si no media su consentimiento inequívoco para ello.

5. El tratamiento de los datos que los distribuidores de seguros lleven a cabo para valorar la honorabilidad comercial y profesional en el marco de lo dispuesto en la ley, deberá limitarse a la exclusiva finalidad de suministro de la información a las Dirección General de Seguros y Fondos de Pensiones, quedando expresamente limitado el número de personas que dentro de la organización pueda tener acceso a dichos datos.

LSSI: A tener en cuenta

ARAG



Los envíos comerciales



Artículo 21 LSSI Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes



1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Los envíos comerciales



Artículo 21. 2. *Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.*

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.



Gracias