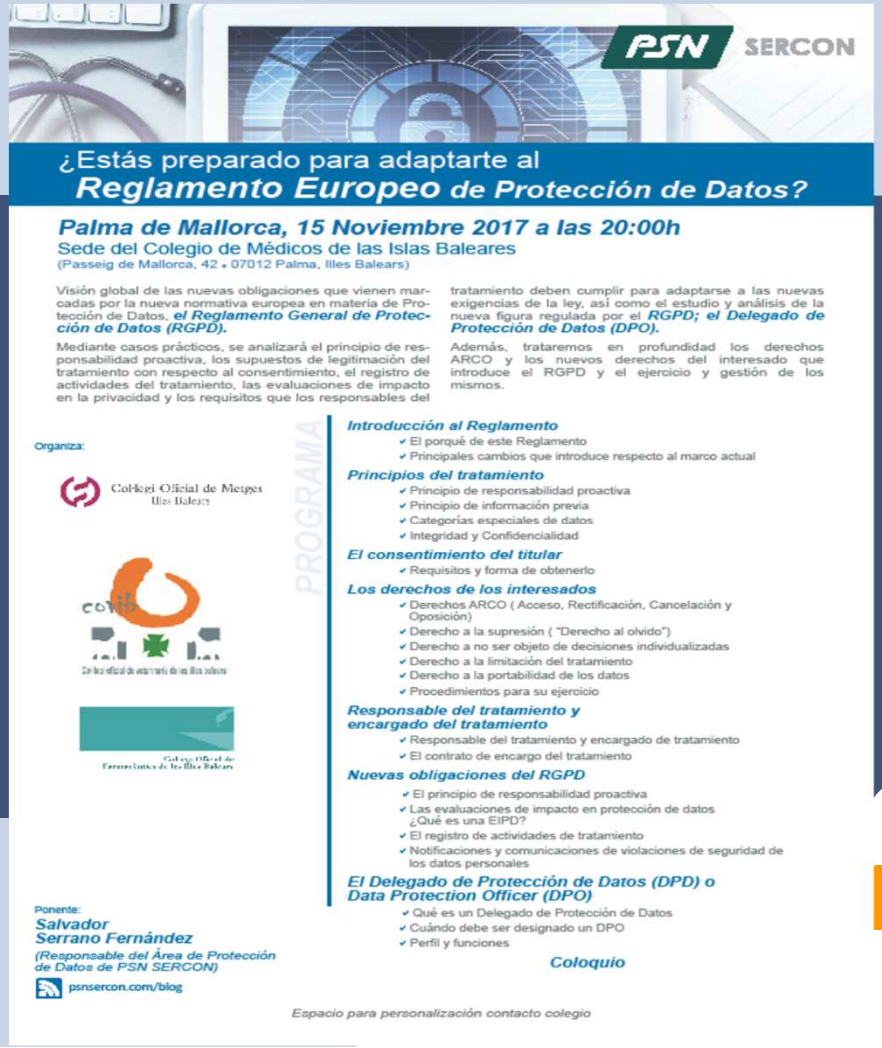
Programa


PSN SERCON
¿Estás preparado para adaptarte al
Reglamento Europeo de Protección de Datos?
Palma de Mallorca, 15 Noviembre 2017 a las 20:00h
Sede del Colegio de Médicos de las Islas Baleares
(Passeig de Mallorca, 42 • 07012 Palma, Illes Balears)
Visión global de las nuevas obligaciones que vienen marcadas por la nueva normativa europea en materia de Protección de Datos, el Reglamento General de Protección de Datos (RGPD).
Mediante casos prácticos, se analizará el principio de responsabilidad proactiva, los supuestos de legitimación del tratamiento con respecto al consentimiento, el registro de actividades del tratamiento, las evaluaciones de impacto en la privacidad y los requisitos que los responsables del tratamiento deben cumplir para adaptarse a las nuevas exigencias de la ley, así como el estudio y análisis de la nueva figura regulada por el RGPD; el Delegado de Protección de Datos (DPO).
Además, trataremos en profundidad los derechos ARCO y los nuevos derechos del interesado que introduce el RGPD y el ejercicio y gestión de los mismos.
Organiza:
Col·legi Oficial de Metges Illes Balears
PROGRAMA
Introducción al Reglamento
El porqué de este Reglamento
Principales cambios que introduce respecto al marco actual
Principios del tratamiento
Principio de responsabilidad proactiva
Principio de información previa
Categorías especiales de datos
Integridad y Confidencialidad
El consentimiento del titular
Requisitos y forma de obtenerlo
Los derechos de los interesados
Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)
Derecho a la supresión ("Derecho al olvido")
Derecho a no ser objeto de decisiones individualizadas
Derecho a la limitación del tratamiento
Derecho a la portabilidad de los datos
Procedimientos para su ejercicio
Responsable del tratamiento y encargado del tratamiento
Responsable del tratamiento y encargado de tratamiento
El contrato de encargo del tratamiento
Nuevas obligaciones del RGPD
El principio de responsabilidad proactiva
Las evaluaciones de impacto en protección de datos ¿Qué es una EIPD?
El registro de actividades de tratamiento
Notificaciones y comunicaciones de violaciones de seguridad de los datos personales
El Delegado de Protección de Datos (DPD) o Data Protection Officer (DPO)
Qué es un Delegado de Protección de Datos
Cuándo debe ser designado un DPO
Perfil y funciones
Coloquio
Ponente:
Salvador Serrano Fernández
(Responsable del Área de Protección de Datos de PSN SERCON)
psnsercon.com/blog
Espacio para personalización contacto colegio

PSN SERCON

Novedades legislativas en Protección de Datos: ¿Estás preparado para adaptarte al Reglamento General de Protección de Datos?

Salvador Serrano Fernández | *Responsable área Protección de Datos PSN SERCON*

GRUPO PSN

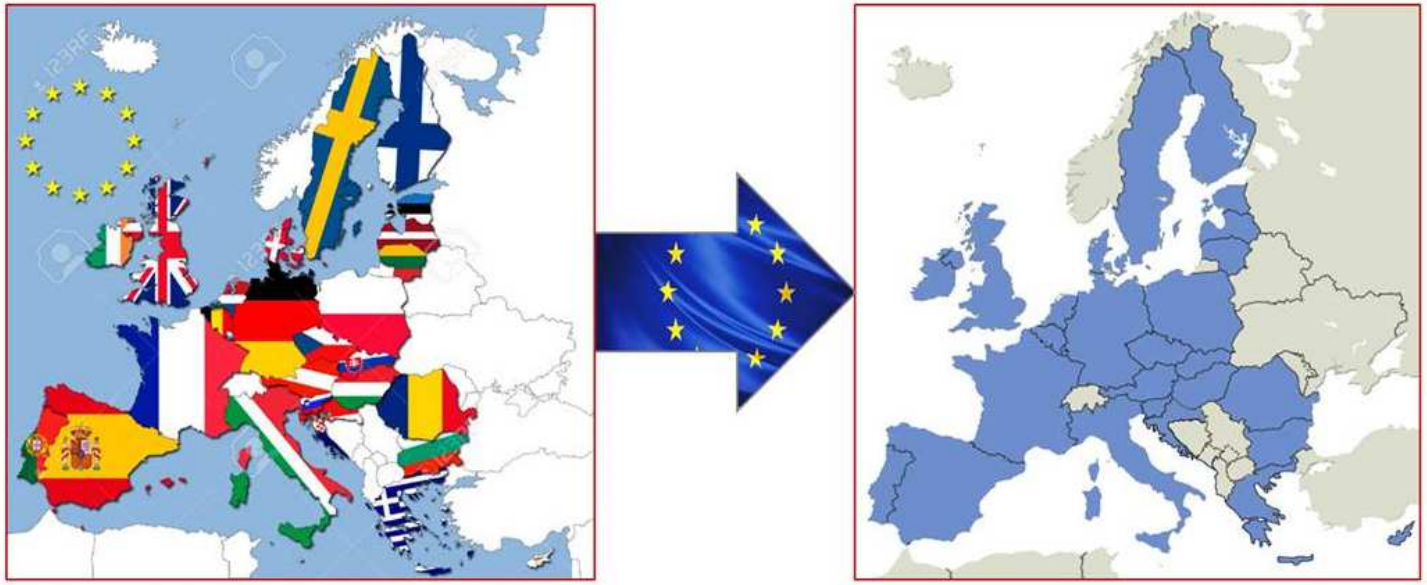
1

INTRODUCCIÓN AL REGLAMENTO

El porqué de este Reglamento y principales cambios respecto al marco actual

> *La legislación siempre va por detrás de los cambios que se producen en la sociedad y le toca adaptarse a la nueva realidad.* ***Las nuevas tecnologías lo han cambiado todo y en muy poco tiempo. En España, la normativa vigente es la Ley Orgánica de Protección de Datos (LOPD) que data de 1999*** *y hace ya* ***17 años de la publicación de esta ley*** *que , ni por asomo, podía avanzar* ***la revolución que iban a traer consigo las nuevas tecnologías*** *y* ***el uso masivo de dispositivos móviles****, redes sociales, compras por Internet…*

GDPR



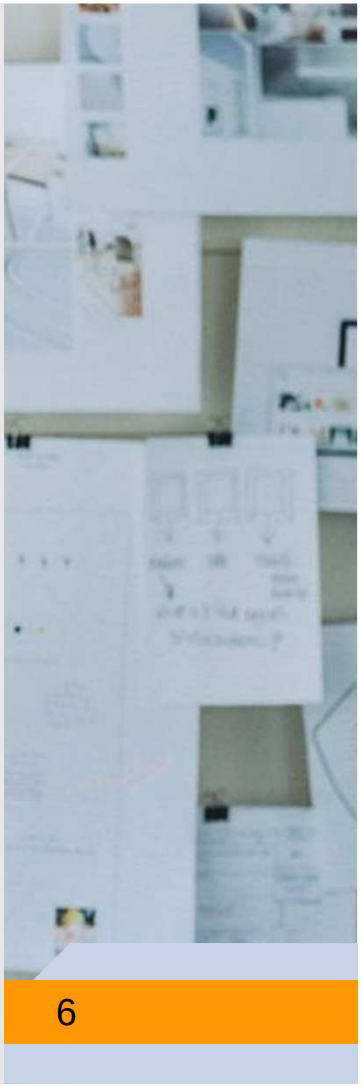
El objetivo de la Comisión Europea ha sido revisar las leyes existentes a la luz del desarrollo tecnológico de los últimos años y el aumento significativo en el tratamiento de datos. También se buscaba una mayor armonización en todos los Estados miembros.

La protección de datos para la era digital en Europa

PSN SERCON

Una protección mejor de los datos personales

- Para el tratamiento de los datos se exige un consentimiento claro
- Más información y más clara sobre el tratamiento
- Derecho a transferir datos de un prestador de servicios a otro
- Limitaciones en el uso del tratamiento automatizado de datos para tomar decisiones, por ejemplo, al elaborar perfiles
- Derecho a rectificar y suprimir datos, incluido el «derecho al olvido» de los datos recogidos en la infancia
- Acceso más fácil a los datos personales
- Derecho a recibir notificación cuando los datos estén comprometidos
- Garantías más estrictas para las transferencias de datos personales fuera de la UE



¿Cuáles son las claves del nuevo Reglamento Europeo de Protección de Datos?

Ámbito

Al ser normativa europea, afecta a **todos los países miembros de la UE**.

Aplicación

También afecta a empresas e instituciones que **no están establecidas en la UE, pero realizan operaciones comerciales en la UE**.

Derecho al olvido y rectificación

Se facilita al ciudadano más elementos de control y medios para ejercerlos.

Consentimiento expreso

Para la utilización de los datos de carácter personal deberás contar con el consentimiento del usuario que debe ser **inequívoco y explícito.**

Responsabilidad proactiva

Adoptar medidas de seguridad para asegurar el cumplimiento de la nueva ley de protección de datos.

Avisos legales

La nueva normativa de protección de datos obliga a **una revisión de las políticas de privacidad que tendrán que explicar la base legal para el tratamiento de los datos**,

2

PRINCIPIOS DEL TRATAMIENTO

Principio de responsabilidad proactiva

Evaluaciones de Impacto sobre la privacidad y Protección de Datos desde el Diseño y por Defecto.

Principio de información previa

Legitimación para el tratamiento de datos y deber de informar.

Categorías especiales de datos

Datos genéticos y datos biométricos que permitan la identificación de una persona.

Integridad y Confidencialidad

Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en las Evaluaciones de Impacto.

PRINCIPIO DE RESPONSABILIDAD PROACTIVA

- Evaluaciones de Impacto.
- Protección de Datos desde el Diseño y por Defecto.

Se deben realizar cuando se prevea que los tratamientos de datos conlleven un alto riesgo para los derechos y libertades de los interesados.

PRINCIPIO DE INFORMACIÓN PREVIA

- Mayor claridad y más información.
- Base legal sobre la que se desarrolla el tratamiento.
- Cambios en los avisos legales y páginas web.

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A. +info…
Finalidad	Gestionar el envío de información y prospección comercial +info…
Legitimación	Consentimiento del interesado +info…
Destinatarios	Otras empresas del grupo Warren&Brandeis, Inc. Encargados de Tratamiento fuera de la UE, acogido a “Privacy Shield” +info…
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional +info…
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos/info/

CATEGORÍAS ESPECIALES DE DATOS

- Tienen la consideración de categorías especiales los datos relativos:

Origen étnico o racial.

Opiniones políticas.

Convicciones religiosas o filosóficas.

Afiliación sindical.

Datos genéticos.

Datos biométricos que permitan la identificación unívoca de una persona.

Datos relativos a la salud.

Datos relativos a la vida y orientación sexuales.

- Obligaciones cuando se tratan categorías especiales de datos:

Prohibición de elaboración de perfiles : Está prohibido el tratamiento basado en una elaboración de perfiles que contemple decisiones individuales basadas en un tratamiento automatizado destinado a evaluar aspectos personales o analizar o predecir datos de salud.

Llevar un Registro de las actividades del tratamiento.

Realizar Evaluaciones de Impacto.

Designar un Delegado de protección de datos (DPO).

INTEGRIDAD Y CONFIDENCIALIDAD

- Aplicar medidas de seguridad como la seudonimización y cifrado de la información.
- Verificar que nuestros proveedores de servicios cumplen con el RGPD a través de los contratos de encargado de tratamiento.
- Si considera o cree que el tratamiento de datos conlleva un riesgo alto, consultar a la autoridad competente (AEPD).

3

EL CONSENTIMIENTO DEL TITULAR

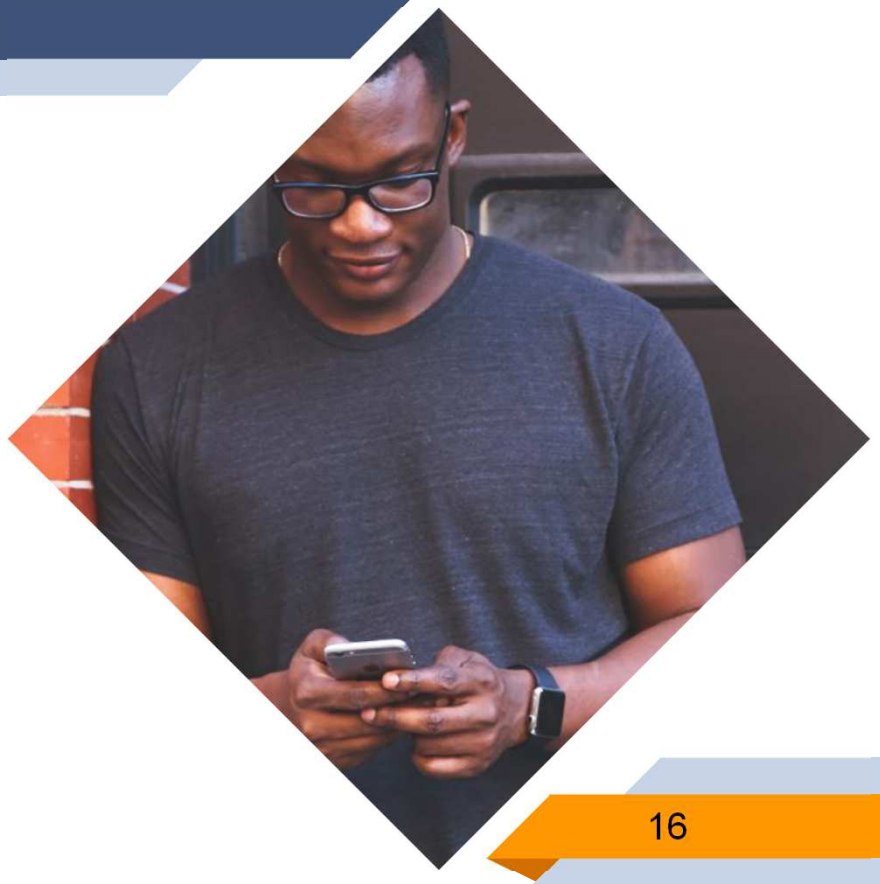
Requisitos y formas de obtenerlo

EL CONSENTIMIENTO DEL TITULAR DE LOS DATOS

El consentimiento tácito o por omisión ya no se admite.

El consentimiento debe ser:

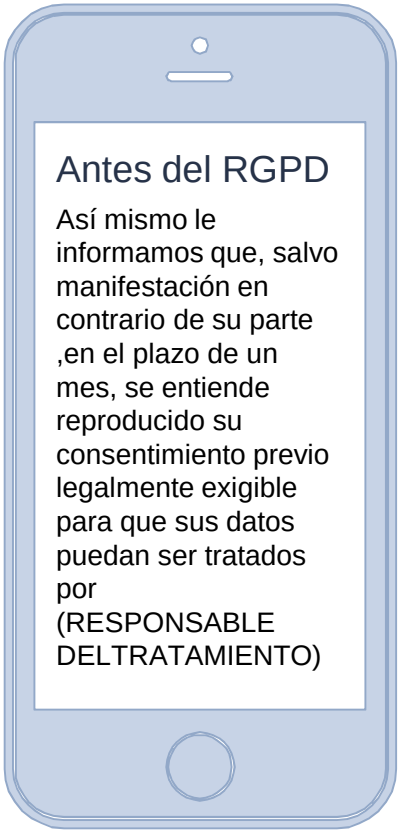
- Explícito
- Inequívoco
- A través de una manifestación del interesado o mediante una clara acción afirmativa.

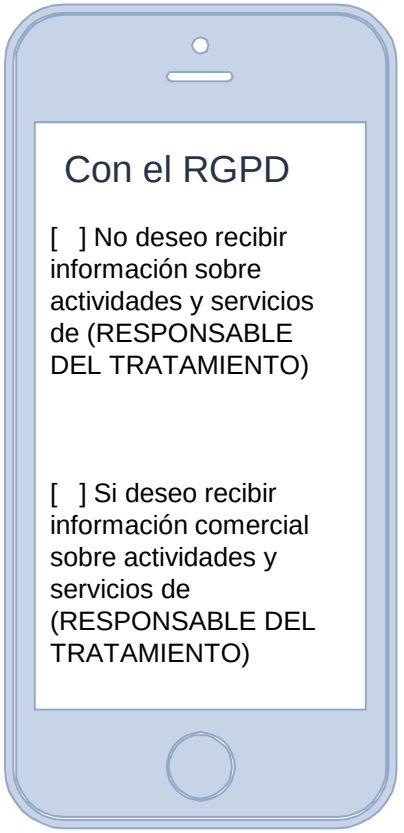


FORMAS DE OBTENER EL CONSENTIMIENTO EN BASE AL RGPD

Mediante la marcación de casillas por parte del interesado.

NOTA: Las casillas pre-marcadas no son válidas.





FORMAS DE OBTENER EL CONSENTIMIENTO EN BASE AL RGPD

En las páginas web una casilla o **“check box”** para marcar con un enlace a la Política de Privacidad.

4

LOS DERECHOS DE LOS INTERESADOS

DERECHOS ARCO Y NUEVOS DERECHOS

Derechos del RGPD	¿En qué consisten tus derechos?
Derecho de acceso	Tienes derecho a que te informen de lo siguiente: → Los fines del tratamiento, categorías de datos personales que se traten y de las posibles comunicaciones de datos y sus destinatarios. → De ser posible, el plazo de conservación de tus datos. De no serlo, los criterios para determinar este plazo. → Del derecho a solicitar la rectificación o supresión de los datos, la limitación al tratamiento, u oponerse al mismo. → Del derecho a presentar una reclamación ante la Autoridad de Control. → Si se produce una transferencia internacional de datos, recibir información de las garantías adecuadas. → De la existencia de decisiones automatizadas (incluyendo perfiles), la lógica aplicada y consecuencias de este tratamiento.
Derecho de rectificación	Tienes derecho, además de rectificar los datos inexactos, a que se completen los datos personales incompletos, inclusive mediante una declaración adicional.
Derecho de supresión (el "Derecho al olvido")	Con este derecho podrás solicitar: → La supresión de los datos personales sin dilación debida cuando concurra alguno de los supuestos contemplados. Por ejemplo, tratamiento ilícito de datos, o cuando haya desaparecido la finalidad que motivó el tratamiento o recogida. → No obstante, se regulan una serie de excepciones en las que no procederá este derecho. Por ejemplo, cuando deba prevalecer el derecho a la libertad de expresión e información.

DERECHOS ARCO Y NUEVOS DERECHOS

Derecho a la limitación del tratamiento	Este derecho te permite: → Solicitar al responsable que suspenda el tratamiento de datos cuando: • Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable. • El interesado ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el interesado. → Solicitar al responsable que conserve tus datos personales cuando: • El tratamiento de datos sea ilícito y el interesado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso • El responsable ya no necesita los datos para los fines del tratamiento pero el interesado si los necesite para la formulación, ejercicio o defensa de reclamaciones.
Derecho a la portabilidad de los datos	Podrás recibir tus datos personales facilitados en un formato estructurado, de uso común y lectura mecánica, y poder transmitirlos a otro responsable, siempre que sea técnicamente posible.
Derecho de oposición	Mediante el derecho de oposición podrás oponerte al tratamiento de tus datos personales: → Cuando por motivos relacionados con tu situación personal, debe cesar el tratamiento de tus datos salvo que se acredite un interés legítimo, o sea necesario para el ejercicio o defensa de reclamaciones. → Cuando el tratamiento tenga por objeto la mercadotecnia directa.

DERECHOS ARCO Y NUEVOS DERECHOS

Derecho a no ser objeto de decisiones individualizadas	Tienes derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos o te afecte. Se exceptúa lo anterior cuando: → Sea necesario para la celebración o ejecución de un contrato. → Esté permitido por el Derecho de la UE o de los Estados miembros, con medidas adecuadas para salvaguardar los derechos y libertades del titular de los datos. → Exista consentimiento explícito del titular de los datos.

Además, el RGPD establece **condiciones concretas sobre el procedimiento** a seguir para atender a los interesados en el ejercicio de sus derechos.

PROCEDIMIENTO PARA EJERCICIO DE DERECHOS

Es obligación de los responsables facilitar a los interesados el ejercicio de sus derechos. Los procedimientos y las formas para ello deben ser **visibles, accesibles y sencillos**. Se requiere que se posibilite la presentación de solicitudes por medios electrónicos.

El ejercicio de los derechos será **gratuito** para el interesado, con la excepción de que se formulen peticiones manifiestamente infundadas o excesivas, en cuyo caso se podrá cobrar un canon de compensación o negarse a actuar.

El **plazo** establecido para responder a las solicitudes será de **un mes, ampliable en caso de especial complejidad de la petición.** El responsable deberá responder en todo caso, y si decide no atender la solicitud deberá informar al interesado en el plazo de un mes, motivando su negativa.

5

RESPONSABLE DEL TRATAMIENTO Y ENCARGADO DEL TRATAMIENTO

RESPONSABLES Y ENCARGADOS DE TRATAMIENTO

- La normativa actual se centra en la actividad de los responsables y ahora ***el RGPD, por el contrario, contiene obligaciones expresamente dirigidas a los encargados de tratamiento (proveedores, gestorías, asesorías, empresas de mantenimiento informático…)***

Responsable del Tratamiento

Encargado del Tratamiento

- Nuevas obligaciones propias que establece el RGPD para los encargados:

  - Deben mantener un **registro de actividades de tratamiento.**
  - Deben determinar **las medidas de seguridad aplicables a los tratamientos** que realizan.
  - Deben designar a un **Delegado de Protección de Datos** en los casos previstos por el RGPD.

LOS CONTRATOS DE ENCARGADO DE TRATAMIENTO

Contrato por escrito

que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas

solo se podrán tratar los datos siguiendo instrucciones del responsable

El tratamiento por el encargado se regirá por **un contrato u otro acto jurídico** con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el **objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales, las categorías de interesados, y los derechos y obligaciones del responsable**.

6

NUEVAS OBLIGACIONES DEL RGPD

EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El RGPD establece un **catálogo de las medidas que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el Reglamento** y estar en condiciones de demostrarlo.

Medidas de	Contratos de encargado de tratamiento	Protección desde el Diseño y por Defecto	Designación de un Delegado de Protección de Datos
responsabilidad proactiva	Evaluaciones de Impacto de Protección de Datos	Registro de actividades de tratamiento	Notificación de violaciones de seguridad de los datos

LAS EVALUACIONES DE IMPACTO EN PROTECCIÓN DE DATOS. ¿QUÉ ES UNA EIPD?

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.

Escalas cualitativas de valoración

Escalas		
Impacto	**Probabilidad**	**riesgo**
MA: muy alto	**MA**: prácticamente seguro	**MA**: crítico
A: alto	**A**: probable	**A**: importante
M: medio	**M**: posible	**M**: apreciable
B: bajo	**B**: poco probable	**B**: bajo
MB: muy bajo	**MB**: muy raro	**MB**: despreciable

Estimación de impacto en la privacidad

IMPACTO EN LOS IPP (PRINCIPIOS DE PRIVACIDAD DE LA INFORMACIÓN)					
NÚM	IPP	E1	E2	E3	E(n)...
1	Informar y recabar el consentimiento.	N/A	BAJO	ALTO	BAJO
2	Limitación en el recabado de datos (adecuados, relevantes y no excesivos).	N/A	BAJO	ALTO	BAJO
3	Tratamiento leal y lícito.	MEDIO	BAJO	BAJO	BAJO
4	Finalidad (limitación en el propósito).	MUY ALTO	MEDIO	MEDIO	MEDIO
5	Calidad de los datos.	MEDIO	MEDIO	BAJO	BAJO
6	Participación individual (acceso, rectificación, cancelación y oposición).	BAJO	BAJO	MEDIO	BAJO
7	Limitación del tiempo de conservación.	BAJO	BAJO	BAJO	MUY ALTO
8	Asegurar un período de retención.	N/A	N/A	N/A	ALTO
9	Seguridad de los datos (Confidencialidad, integridad y disponibilidad).	ALTO	N/A	ALTO	ALTO
10	Transparencia (Políticas y procedimientos claros y conocidos).	MUY ALTO	BAJO	BAJO	MEDIO

EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

PSN SERCON

NOTIFICACIONES TELEMATICAS A LA AEPD

Inscripción de Ficheros

Basado en el sistema NOTA de declaración de ficheros

EXENTO

para empresas y organizaciones que empleen a menos de 250 trabajadores

EXCEPCIÓN : 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

Responsables y encargados deberán **mantener un registro de actividades de tratamiento** en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable y del Delegado de Protección de Datos si existiese
- Finalidades del tratamiento
- Descripción de categorías de interesados y categorías de datos personales tratados
- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales
- Transferencias internacionales de datos y descripción general de las medidas técnicas y organizativas de seguridad

NOTIFICACIONES Y COMUNICACIONES DE VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

- ***El RGPD*** define las violaciones de seguridad de los datos, más comúnmente conocidas como ***"quiebras de seguridad",*** de una forma muy amplia, que incluye ***todo incidente 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.***

- Cuando se produzca una violación de la seguridad de los datos, ***el responsable debe notificarla a la autoridad de protección de datos competente dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.***

La notificación ha de incluir un contenido mínimo:

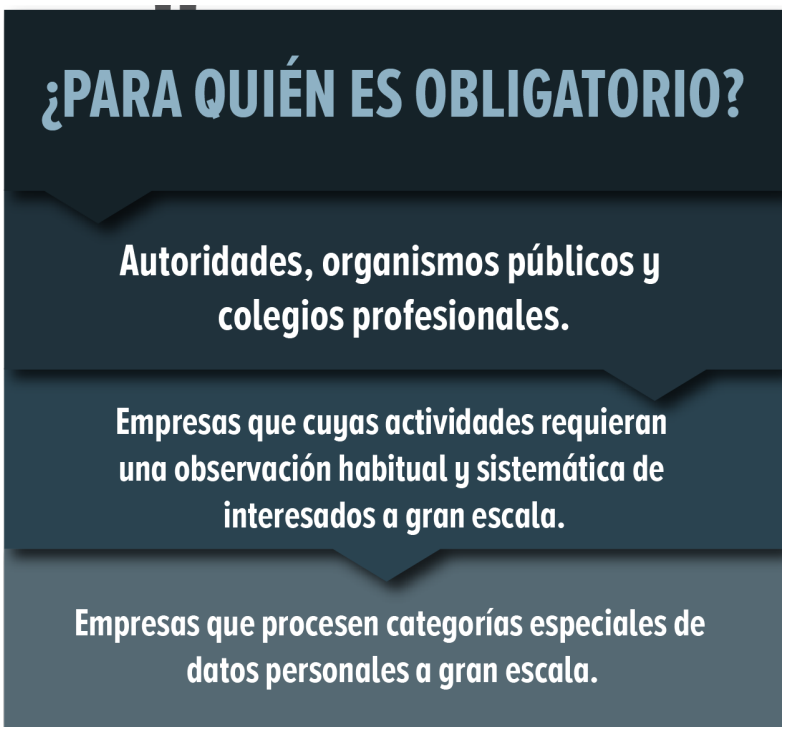
- la naturaleza de la violación.
- categorías de datos y de interesados afectados.
- medidas aplicadas para solventar la quiebra y los posibles efectos negativos sobre los interesados

7

EL DELEGADO DE PROTECCIÓN DE DATOS

¿QUÉ ES UN DELEGADO DE PROTECCIÓN DE DATOS (DPO)?

¿PARA QUIÉN ES OBLIGATORIO EL DELEGADO DE PROTECCIÓN DE DATOS (DPO) ?



PERFIL DEL DELEGADO DE PROTECCIÓN DE DATOS (DPO)

REQUISITOS

PROFESIONAL ESPECIALIZADO EN DERECHO Y PROTECCIÓN DE DATOS Y CON EXPERIENCIA PRÁCTICA EN LA MATERIA.

LA INDEPENDENCIA DEL DPO DEBE ESTAR GARANTIZADA.

SE PERMITE LA EXTERNALIZACIÓN DEL SERVICIO.

INCOMPATIBILIDADES

PERSONAS QUE PUEDAN GENERAR CONFLICTO DE INTERESES COMO PUESTOS DE ALTA DIRECCIÓN U OTRAS POSICIONES CON RESPONSABILIDAD SOBRE LA DETERMINACIÓN DE PROPÓSITOS Y MEDIOS DE PROCESAMIENTO.

¿CUANDO DEBE SER DESIGNADO EL DELEGADO DE PROTECCIÓN DE DATOS (DPO) ?

- Colegios profesionales y Consejos Generales.
- Centros Docentes que ofrezcan enseñanzas regladas.
- Universidades públicas y privadas.
- Entidades que exploten redes y presten servicios de comunicaciones
- Las empresas de servicios de inversiones.
- Actividades de Seguridad Privada.
- Entidades de comunes de la solvencia patrimonial y crédito.
- Prestadores de servicios de la sociedad de la información.
- Entidades de crédito y los establecimientos financieros de crédito.
- Los operadores que desarrollen la actividad de juego.
- 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.
- Los centros sanitarios
  Los centros obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre.

PSN SERCON

- **Designación voluntaria**

Los responsables o encargados del tratamiento no incluidos en el listado anterior podrán designar un Delegado de Protección de Datos de forma voluntaria.

FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS (DPO)

PSN SERCON

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

8

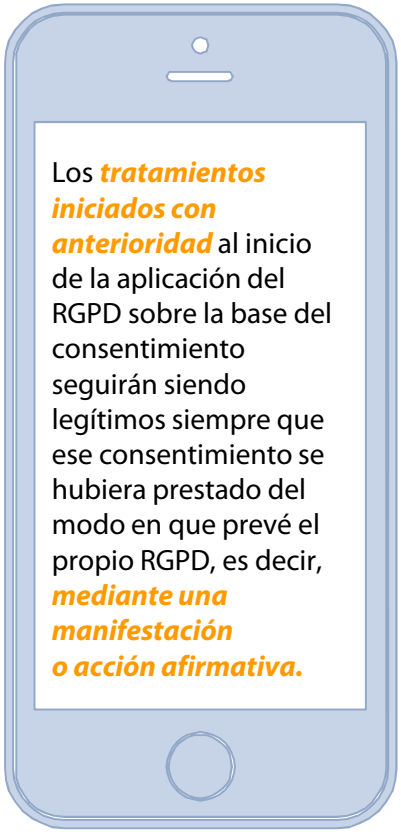
PREGUNTAS FRECUENTES

¿QUIÉN PUEDE SER DPO?

El **DPO** ha de ser nombrado atendiendo a sus ***cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos.***

Debe ser un **profesional especializado en Derecho y experiencia profesional demostrable en materia de protección de datos y conocimiento profundo del RGPD** en la medida en que las funciones del DPO incluye el **asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos**, por ello, los **conocimientos jurídicos en la materia son sin duda necesarios.**

¿TENGO QUE RECABAR TODOS LOS CONSENTIMIENTOS POR ESCRITO CON ANTERIORIDAD A LA NUEVA LEY?



¿QUE PUEDE SUCEDERME SI NO ESTOY PREPARADO ANTES DEL 25 DE MAYO DEL 2018?

Norma aplicable	Sanciones		
	Leve	Grave	Muy grave
RGPD	No se establece un rango mínimo de cuantía	Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.	Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.

MUCHAS GRACIAS
POR SU ATENCIÓN.

SI QUIERE ESTAR AL DÍA Y MANTENERSE INFORMADO RESPECTO A NOVEDADES SOBRE PROTECCIÓN DE DATOS, PUEDE VISITAR NUESTRO BLOG:

https://blog.psnsercon.com/

@GRUPOPSN GRUPO PSN GRUPO PSN GRUPO PSN HTTP://BLOG.PSN.ES

PSN SERCON GRUPO PSN