

# EL IMPACTO DE LA NUEVA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS EN NUESTRO SECTOR “EL SALÓN DE JUEGO”



10.05.2018

1. **Presentación.**

- **Jesús Martín Sanz.** <https://es.linkedin.com/in/jesús-martín-sanz-22102316>

**Consultor en estrategia empresarial y formación.**

- **Rafael Andrés Álvez.** <https://www.linkedin.com/in/rafael-andr%C3%A9s-alvez-89336b11/>

**Abogado especialista en derecho administrativo deportivo y del juego.**

- **Santiago Vecina Cabeza.** <https://es.linkedin.com/in/santiago-vecina-cabeza-a2821821>

**Consultor en Sector del Juego, Estrategia y Desarrollo de Negocio.**

2. **Objetivos**

3. **Diagnóstico y estrategia empresarial ante la nueva normativa.**

- **Efectos de la regulación en la empresa.**
- **Gestión del riesgo normativo.**
- **DAFO de la empresa ante la RGPD.**
- **CAPA de la empresa para afrontar la RGPD.**
- **Estrategia empresarial para el nuevo escenario.**
- **El papel de DataPro Asesores para las empresas.**

### **3. Análisis técnico-jurídico del RGPD.**

- **Entrada en vigor y principios generales.**
- **Proactividad y prueba.**
- **Consentimiento.**
- **Transparencia en la información.**
- **Responsabilidad encargado del tratamiento.**
- **Seguridad desde “el diseño y por defecto”.**
- **Registro de Actividad de Tratamiento.**
- **Nuevos derechos mayor control.**
- **El Delegado de Protección de Datos.**
- **Régimen sancionador.**

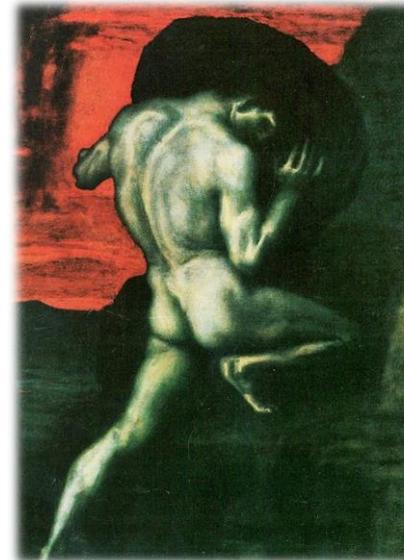
### **4. Hoja de ruta recomendada por DataPro Asesores para empresas titulares de Salones de Juego.**

## Objetivos

- 1. Conocimiento de las modificaciones, en las normas reguladoras de Protección de Datos.**
- 2. Análisis del nuevo marco de obligaciones impuesto a la empresa.**
- 3. Detección del grado de cumplimiento normativo de la empresa y adecuación del mismo al RGPD.**

## Efectos de la regulación en la empresa

- Carga administrativa.
- Costes estructurales.
- Consumo de recursos.
- Integración procedimientos.
- Pérdida de márgenes.



# Gestión del riesgo normativo



**Conocimiento del riesgo**



**Tratamiento del riesgo**



**Transferencia del riesgo**

## DAFO de la empresa ante el RGPD

Debilidades	Amenazas
<ul style="list-style-type: none"> <li>• Desconocimiento de la nueva normativa.</li> <li>• Falta de experiencia en su gestión.</li> <li>• No disponibilidad de recursos ociosos para el RGPD.</li> <li>• Sistemas no integrados o dificultades para integrar uno más.</li> </ul>	<ul style="list-style-type: none"> <li>• Normativa confusa y de difícil interpretación.</li> <li>• Discrecionalidad del regulador en la inspección y resolución.</li> <li>• Sistemas de minería de datos en constante evolución y BBDD cambiantes en el tiempo: campos, registros, datos, etc.</li> <li>• Cambios normativos europeos y adaptaciones diferentes por las distintas administraciones.</li> </ul>
Fortalezas	Oportunidades
<ul style="list-style-type: none"> <li>• Empresas con prácticas en sistemas de regulación, experiencia en procedimientos de calidad, prevención, compliance, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Profesionalizar las BBDD.</li> <li>• Integrar y digitalizar los sistemas de regulación en la empresa.</li> <li>• Mejorar la RSC y reputación.</li> </ul>

## CAPA de la empresa para afrontar el RGPD

Superar las Debilidades	Blindarse de las Amenazas
<ul style="list-style-type: none"> <li>• <b>Plan de Formación</b> para superar el Desconocimiento.</li> <li>• <b>Plan de Asesoramiento</b> para superar la Falta de experiencia.</li> <li>• <b>Externalizar la gestión del RGPD</b> ante la No disponibilidad de recursos.</li> <li>• <b>Plan de integración de los Sistemas regulatorios</b> que afectan a la empresa.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Asesorarse para evitar la confusión e interpretaciones erróneas.</b></li> <li>• <b>Asesorarse para optimizar la comunicación con el regulador</b> en la inspección y resolución.</li> <li>• <b>Externalizar para gestionar los cambios</b> de Sistemas de minería de datos y BBDD cambiantes en el tiempo: campos, registros, datos, etc. Y los Cambios normativos europeos y de distintas administraciones.</li> </ul>
Utilizar las Fortalezas	Aprovechar las Oportunidades
<ul style="list-style-type: none"> <li>• <b>Utilizar la experiencia y homogeneizar</b> los sistemas de regulación, procedimientos de calidad, prevención, compliance, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Profesionalizar las BBDD.</b></li> <li>• <b>Integrar y digitalizar los sistemas de regulación</b> en la empresa.</li> <li>• <b>Mejorar la RSC y reputación.</b></li> </ul>

## Estrategia empresarial para el nuevo escenario

- **Plan de Asesoramiento.**
- **Plan de Formación a empleados.**
- **Externalización de la gestión del RGPD.**
- **Plan de integración y digitalización de los Sistemas regulatorios.**
- **Profesionalizar la gestión de las BBDD.**
- **Mejorar la RSC y reputación.**

## El papel de DataPro Asesores para las empresas

- 1. Asesoramiento permanente, en modo online y telefónico.**
- 2. Formación: Cursos online, opcionalmente bonificables por FUNDAE.**
- 3. Externalización de la gestión del RGPD.**

# Entrada en vigor y principios generales

- **El RGPD será aplicable a partir del 25 de mayo de 2018.**
- Se deberá aplicar también la legislación estatal (LOPD y su Reglamento -RD 1720/2007-) y autonómica sobre protección de datos, en lo que no contravenga el RGPD.
- Seguirá siendo válido todo lo que se haya derivado de las interpretaciones sobre las que se apoyan las resoluciones, los informes y las recomendaciones de la AEPD y las sentencias que hayan sido dictadas.
- Así mismo, a día de hoy, se encuentra en desarrollo la nueva Ley Orgánica española, en esta materia.



## Proactividad y prueba

- Como idea fundamental, **el RGPD obedece al principio de responsabilidad proactiva** que requiere que las Organizaciones analicen:
  - qué datos tratan,
  - con qué finalidades lo hacen y
  - qué tipo de operaciones de tratamiento llevan a cabo
- Y a partir de este análisis, determinar la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que:
  - **pueden demostrarlo ante los interesados y**
  - **ante la Agencia Española de Protección de Datos**

## Consentimiento

- Es uno de los cambios más relevantes que implica el RGPD.
- Sólo se podrá obtener mediante **una declaración expresa de los interesados o una acción positiva que indique el acuerdo del mismo.**
- **El consentimiento debe ser inequívoco, libre, específico, revocable, informado, claro y distinguible.**

## Consentimiento

- La obtención del consentimiento SIEMPRE debe estar **documentada**. Hay que saber ¿Quién consintió? ¿Cuándo consintió? ¿Qué información recibió? ¿Cómo se consintió? Y si se hubiera revocado el consentimiento.
- El consentimiento deberá recabarse ANTES DE INICIAR CUALQUIER TRATAMIENTO, estará **limitado** en el tiempo y depende de su objeto y contexto.

## Transparencia en la información

Se deberán revisar las cláusulas informativas, respecto a la política de privacidad y cookies así como los avisos legales. Principio de Transparencia. El RGPD obliga a incorporar en la información que se proporciona a los interesados una serie de cuestiones que antes no eran obligatorias:

### Art 5 LOPD

- Finalidad.
- Destinatarios ficheros.
- Obligación o no de la entrega y sus consecuencias.
- Los derechos del interesado.
- La identidad del responsable.

### Art 12 RGPD

- Base jurídica del tratamiento.
- Tiempo máximo que se tendrán datos.
- Identificación DPD, en su caso.
- Si hay o no transferencia internacional.
- Derecho a presentar reclamación.
- Existencia o no de decisiones automatizadas y perfiles.

## Transparencia en la información

Esta información :

- Deberá darse de forma concisa, transparente, inteligible, con un lenguaje claro y sencillo.
- Su acceso deberá ser fácil.
- Por escrito u otros medios y de forma gratuita.

## Responsabilidad encargado del tratamiento

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste. En nuestro caso fundamentalmente proveedores de servicios (administrativos, consultoría, web, etc.).

El responsable del tratamiento debe elegir un encargado del tratamiento **que ofrezca garantías suficientes** respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del encargado:

- Código de Conducta: elemento recomendado por el RGPD.
- Certificación.

## Responsabilidad encargado del tratamiento

### **El Encargado de Tratamiento. Cláusulas específicas en sus contratos.**

Se amplía el contenido de los **contratos firmados** con los encargados de tratamiento que, siempre **deberán constar por escrito** y deberán incluir, entre otros aspectos:

- Objeto, duración, naturaleza, finalidad del tratamiento, tipo de datos y categoría interesados.
- Confidencialidad.
- Destino de los datos tras finalizar la prestación del encargo.
- Instrucciones del responsable y descripción detallada de los servicios prestados y colaboración en las obligaciones del responsable (derechos interesados y cumplimiento).
- Medidas de seguridad aplicadas.
- Posibles transferencias internacionales de datos.
- Subcontrataciones.

Es recomendable revisar los contratos para adecuarlos o firmar de nuevo con todos los proveedores de servicios nuevos contratos con el contenido adaptado al RGPD.

## Seguridad desde “el diseño y por defecto”

- **Responsabilidad proactiva.**
- Protección de datos **desde el diseño y por defecto** lo que implica:
  - Aplicar garantías necesarias de protección de datos desde la fase inicial de planificación de cualquier herramienta que se vaya a utilizar para procesar datos.
  - Si hay varias configuraciones de privacidad en los elementos con los que tratemos datos se deberán escoger aquellas que ofrezcan más garantías lo que implicara siempre la minimización de datos, el riguroso control de acceso, el establecimiento de plazos de conservación y la transparencia en la información.



— Adecuar los **FORMULARIOS** *derecho de información*



— Elaborar / Adaptar **POLÍTICA DE PRIVACIDAD**



— Adaptar los **MECANISMOS Y PROCEDIMIENTOS** para el ejercicio de derechos

## Seguridad desde “el diseño y por defecto”

- **Medidas de seguridad (técnico-organizativas):**

Se ha de **asegurar la confidencialidad, integridad, disponibilidad, y resiliencia** de los sistemas y servicios de tratamiento. En su caso, seudonimización y cifrado.

**Evitar riesgos** de destrucción, pérdida o alteración accidental o ilícita en el tratamiento, transmisión y conservación.

Verificar y **evaluar las medidas de manera periódica:**

- **Análisis de riesgos y evaluaciones de impacto** (cuando sea probable que el tratamiento presente un alto riesgo específico para los derechos y libertades de los interesados-elaboración perfiles tratamiento masivo datos sensibles).

## Seguridad desde “el diseño y por defecto”

- Actuaciones concretas:
  - Registro de Actividad de Tratamiento, DPD y Punto centralizado (en caso de empresas multi sede, sería la Sede elegida para el tratamiento de datos), en su caso.
  - Notificación de violaciones de la seguridad de los datos.
  - Proyección de información de las políticas de privacidad de datos y formación a los empleados.
  - Transferencias internacionales.

Estas medidas deben implementarse de acuerdo con el estado de la técnica, los costes de aplicación, la naturaleza contexto, alcance y finalidades del tratamiento así como tener en cuenta los riesgos y probabilidad para los derechos y libertades de los interesados.

## Registro de Actividad de Tratamiento

La actual inscripción de ficheros ante la AEPD desaparece, al igual que el Documento de Seguridad, exigido en el reglamento de desarrollo de la LOPD y en el que se establecen los niveles de seguridad básico, medio y alto.

Ahora se obliga al responsable de tratamiento (RT) y al encargado de tratamiento (ET) a llevar un Registro de actividades de tratamiento con un contenido mínimo (Art 30 RGPD):

### **Responsable del tratamiento:**

- Datos de contacto de todos los implicados en el tratamiento.
- Fines del tratamiento
- Descripción de las categorías de interesados
- Descripción de las categorías de datos
- Categorías de Destinatarios.
- Transferencias internacionales de datos y documentación de garantías apropiadas.
- Cuando sea posible:
  - Plazos previstos para suprimir las categorías de datos.
  - Descripción de las medidas técnicas y organizativas de seguridad.

## Registro de Actividad de Tratamiento

### Encargado del tratamiento:

- Datos de contacto de todos los implicados en el tratamiento.
- Categorías de datos y de tratamiento efectuados en nombre de cada Responsable del tratamiento.
- Transferencias internacionales de datos y documentación de garantías apropiadas.
- Cuando sea posible, una descripción de las medidas técnicas y organizativas de seguridad.

## Registro de Actividad de Tratamiento

Este registro no es obligatorio en empresas menores de 250 trabajadores excepto si se tratan datos que:

- Pueda entrañar un riesgo para los derechos y libertades de los interesados, categorías especiales de datos personales (indicadas en el artículo 9 del RGPD) sean relativos a condenas e infracciones penales, **o se traten de manera no ocasional**. Categorías especiales:
  - Origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas.
  - Afiliación sindical.
  - 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 orientaciones sexuales de una persona física.

Se deben mantener por **escrito** valiendo también formato electrónico, actualizado y a disposición de la AEPD.

# Registro de Actividad de Tratamiento

## OPERACIONES EN CONDICIÓN DE RESPONSABLE DE TRATAMIENTO

<b>Fichero o Colectivo objeto de tratamiento</b>	<b>CLIENTES</b>
<b>Categoría de interesados</b>	Clientes y usuarios, personas de contacto
<b>Tipología de datos</b>	Nif, nombre y apellidos, dirección, teléfono, e-mail, firma, económicos, financieros y seguros, transacciones de bienes y servicios y otras categorías especiales de datos
<b>Finalidad del tratamiento</b>	Gestión de clientes, contables, fiscal y administrativa, publicidad y prospección comercial, educación
<b>Categorías de destinatarios</b>	Agencia Tributaria, Seguridad Social, Bancos y Cajas
<b>Transferencia internacional</b>	No prevista
<b>Medidas técnicas y organizativas</b>	Protocolos para el cumplimiento de las medidas de seguridad" del documento Medidas y Procedimientos de.....
<b>Plazos de supresión</b>	Los legalmente establecidos

# Registro de Actividad de Tratamiento

## OPERACIONES EN CONDICIÓN DE RESPONSABLE DE TRATAMIENTO

<b>Fichero o Colectivo objeto de tratamiento</b>	<b>PROVEEDORES</b>
<b>Categoría de interesados</b>	Proveedores
<b>Tipología de datos</b>	Información comercial, Nif, nombre y apellidos, dirección, teléfono, e-mail, firma
<b>Finalidad del tratamiento</b>	Gestión de clientes, contable, fiscal y administrativa, otras finalidades
<b>Categorías de destinatarios</b>	Agencia Tributaria y bancos y cajas
<b>Transferencia internacional</b>	No prevista
<b>Medidas técnicas y organizativas</b>	Protocolos para el cumplimiento de las medidas de seguridad" del documento Medidas y Procedimientos de.....
<b>Plazos de supresión</b>	Los legalmente establecidos

# Registro de Actividad de Tratamiento

## OPERACIONES EN CONDICIÓN DE RESPONSABLE DE TRATAMIENTO

<b>Fichero o Colectivo objeto de tratamiento</b>	<b>RECURSOS HUMANOS</b>
<b>Categoría de interesados</b>	Solicitantes, empleados, personas que entregan el currículum a la empresa
<b>Tipología de datos</b>	Nif, nombre y apellidos, dirección, teléfono, e-mail, firma, características personales, académicos y profesionales, detalles de empleo
<b>Finalidad del tratamiento</b>	Gestión de recursos humanos de la entidad
<b>Categorías de destinatarios</b>	No prevista ninguna cesión
<b>Transferencia internacional</b>	No prevista
<b>Medidas técnicas y organizativas</b>	Protocolos para el cumplimiento de las medidas de seguridad" del documento Medidas y Procedimientos de.....
<b>Plazos de supresión</b>	Los legalmente establecidos

# Registro de Actividad de Tratamiento

## OPERACIONES EN CONDICIÓN DE RESPONSABLE DE TRATAMIENTO

<b>Fichero o Colectivo objeto de tratamiento</b>	<b>USUARIOS WEB</b>
<b>Categoría de interesados</b>	Clientes y usuarios, usuarios de la página web y perfiles en redes sociales
<b>Tipología de datos</b>	Nif, nombre y apellidos, dirección, teléfono, e-mail, información comercial y otras categorías especiales de datos
<b>Finalidad del tratamiento</b>	Análisis de perfiles, publicidad y prospección comercial, prestación de servicios de comunicaciones electrónicas, comercio electrónico, prestación de servicios de certificación electrónica
<b>Categorías de destinatarios</b>	Organizaciones o personas directamente relacionadas con el responsable

## Nuevos derechos, mayor control

### Los derechos de los titulares de datos:

- La LOPD reconocía los denominados derechos ARCO (acceso, rectificación, cancelación y oposición).
- El RGPD introduce tres nuevos derechos: **Olvido, portabilidad y limitación de tratamiento.**
- El **responsable deberá informar al interesado** sobre las actuaciones derivadas de su petición en el plazo de **un mes** que podría ampliarse hasta dos, si el responsable decidiera no atender una solicitud deberá informar de la negativa en un plazo de un mes.

## Nuevos derechos, mayor control

### Brechas de seguridad

Brecha de seguridad: es toda violación 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 autorizado a dichos datos.

Establecer mecanismos y procedimiento de NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

**Comunicar SIEMPRE sin dilación indebida a la AEPD en plazo límite de 72 horas desde su constancia a la AEPD salvo que** “sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas”. Art 33.1 RGPD.

**Si la violación entraña un grave riesgo para las libertades y derechos de los usuarios también debe comunicarse a éstos.**

## El Delegado de Protección de Datos

Se designará un delegado de protección de datos siempre que:

- a) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
- b) Las **actividades principales** del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una **observación habitual y sistemática** de interesados **a gran escala**.
- c) Las **actividades principales** del responsable o del encargado consistan en el tratamiento **a gran escala de categorías especiales de datos personales** y de datos relativos a condenas e infracciones penales.

# El Delegado de Protección de Datos



**OPERADORES  
DE JUEGO  
ELECTRÓNICO**



**CENTROS  
SANITARIOS**



**PUBLICIDAD Y  
PROSPECCIÓN  
COMERCIAL**



**SERVICIOS  
COMUNICACIONES  
ELECTRÓNICAS**



**SERVICIOS DE LA  
SOCIEDAD DE LA  
INFORMACIÓN**



**ENTIDADES DE  
CRÉDITO**



**FOMENTO  
FINANCIACIÓN  
EMPRESARIAL**



**EMPRESAS DE  
SEGURIDAD  
PRIVADA**



**SERVICIOS DE  
INVERSIÓN**



**SOLVENCIA  
PATRIMONIAL Y  
CRÉDITO**



**DISTRIBUIDOR  
ELECTRICIDAD**



**CENTROS  
DOCENTES**



**COLEGIOS  
PROFESIONALES**



**EMISORES DE  
INFORMES  
COMERCIALES**



**ENTIDADES  
ASEGURADORAS**

## El Delegado de Protección de Datos

El DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados en Derecho y la práctica en materia de protección de datos.

Es importante tener en cuenta, en relación con la obligación de nombrar un DPD (cuando sea exigible) que:

- Se permite nombrar **un solo DPD para un grupo empresarial**, que mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios y desarrolle sus funciones a tiempo completo o parcial.
- Debe participar **de forma adecuada y en tiempo oportuno** en todas las cuestiones relativas a la protección de datos personales.

## El Delegado de Protección de Datos

- Debe participar **de forma adecuada y en tiempo oportuno** en todas las cuestiones relativas a la protección de datos personales.
- Debe recibir el **apoyo del responsable o encargado**, que deberán facilitarle los recursos necesarios para el desempeño de sus funciones.
- **No debe recibir ninguna instrucción en lo que respecta al desempeño de dichas funciones** y no ser destituido ni sancionado por el responsable o el encargado por causas relacionadas con ese desempeño de funciones.
- Deberá rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado. Esta característica debe interpretarse en el sentido de que el DPD debe poder relacionarse con niveles jerárquicos que tengan la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones que realice el DPD.

# El Delegado de Protección de Datos

## Funciones DPD

- Informar, asesorar y sensibilizar al responsable de la empresa y trabajadores sobre el cumplimiento de la normativa.
- **Supervisar la implantación** y aplicación de las políticas de protección de datos en la empresa.
- **Atender las peticiones de información de los interesados** en el ejercicio de sus derechos de conformidad con la legislación de protección de datos.
- **Velar por la documentación** que contenga datos personales.
- Supervisar la documentación, notificación y comunicación.
- De las violaciones de datos personales de conformidad con la normativa.

DPD

# El Delegado de Protección de Datos

## Funciones DPD

- Supervisar la **Evaluación de Impacto de Protección de Datos**.
- **Supervisar la respuesta** a las solicitudes de la AEPD.
- **Actuar como punto de contacto para la AEPD**.
- **Comprobar la conformidad del tratamiento cuando sea necesario realizar una consulta previa a la AEPD**.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Castellano Català

Buscar...

TRANSPARENCIA: LA AGENCIA    CANAL DEL CIUDADANO    CANAL DEL RESPONSABLE    RESOLUCIONES Y DOCUMENTOS    FICHEROS INE

**La AEPD publica un sistema de notificación electrónica para comunicar la designación de Delegados de Protección de Datos**

El RGPD establece que los responsables o encargados del tratamiento deben publicar los datos de contacto de su DPD y comunicarlos a la autoridad de control

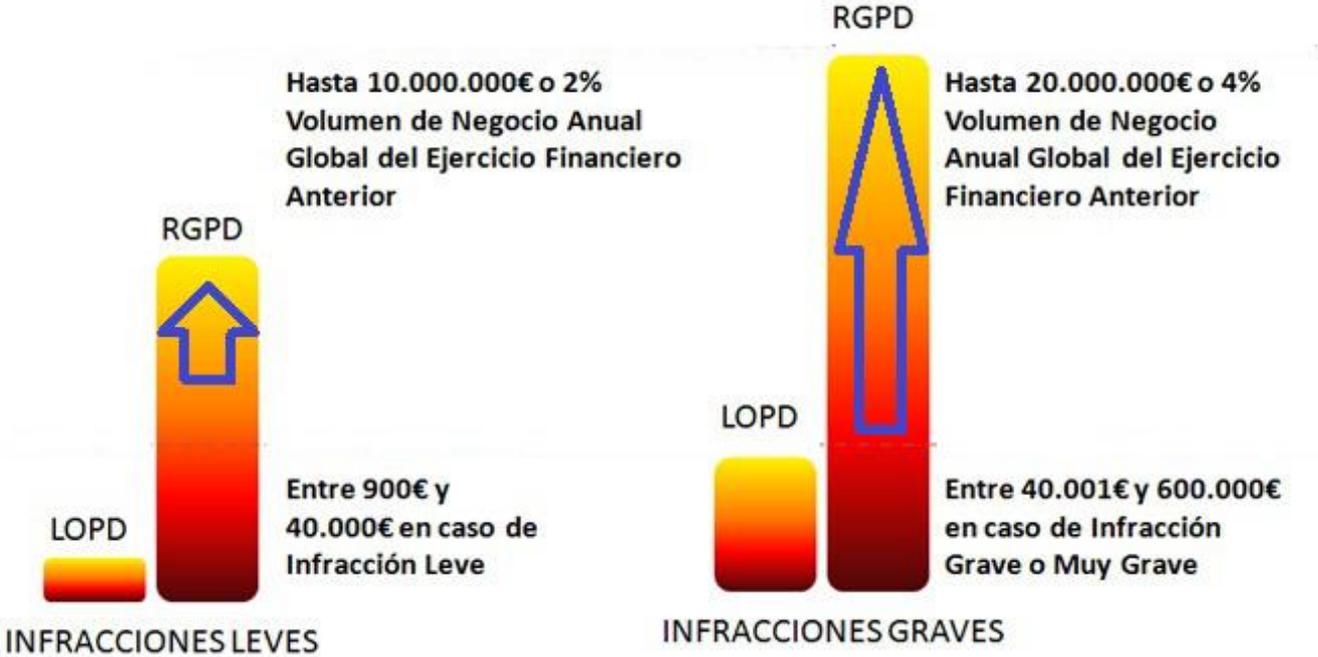
[Formulario online](#)

1

The screenshot shows the official website of the Spanish Data Protection Agency (AEPD). The header includes the agency's name and logo, along with language options for Castellano and Català, and a search bar. A navigation menu lists various services like 'TRANSPARENCIA: LA AGENCIA', 'CANAL DEL CIUDADANO', 'CANAL DEL RESPONSABLE', 'RESOLUCIONES Y DOCUMENTOS', and 'FICHEROS INE'. The main content area features a news article with a title in orange: 'La AEPD publica un sistema de notificación electrónica para comunicar la designación de Delegados de Protección de Datos'. Below the title, a paragraph explains that the RGPD requires data controllers to publish their Data Protection Delegates' contact information to the authority. An orange link 'Formulario online' is provided. To the right of the text is an illustration of a person with glasses working on a laptop, with a stopwatch, gears, and a bar chart in the background.

# Régimen sancionador

Dependiendo del artículo del Reglamento General de Protección de Datos que haya sido vulnerado, y sin perjuicio del **derecho de indemnización que el Interesado pudiera reclamar judicialmente**, las sanciones impuestas sobre infracciones al RGPD pueden ascender de los 10 millones de euros (o el 2% como máximo del volumen de negocio total anual global) **hasta los 20 millones de euros** (o el 4% como máximo del volumen de negocio total anual global).



## Hoja de Ruta recomendada para empresas titulares de Salones de Juego

1. Designar DELEGADO DE PROTECCIÓN DE DATOS (DPD), si es obligatorio para la empresa o si lo asume voluntariamente. En caso de no ser necesario designar un DPD, cuando menos identificar a la/s persona/s responsables de COORDINAR LA ADAPTACIÓN.
2. Realizar un ANÁLISIS DE RIESGOS. Actualizar Procedimientos y BBDD existentes, recabando el consentimiento expreso del afectado.
3. Elaborar el REGISTRO ACTIVIDADES DE TRATAMIENTO teniendo en cuenta su finalidad y la base jurídica.
4. Revisar MEDIDAS DE SEGURIDAD a la luz de los resultados del análisis de riesgos.
5. Establecer mecanismos y procedimiento de NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD.

## Hoja de Ruta recomendada para empresas titulares de Salones de Juego

6. A partir de los resultados del análisis de riesgos, realizar, en su caso, una **EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS**.
7. **FORMAR AL PERSONAL**, en materia de Protección de Datos.
8. Revisar y adecuar formularios y consentimientos.
9. Adaptar contratos con terceros.
10. Adaptar políticas y procedimientos.

**GRACIAS**

**Santiago Vecina Cabeza**

**[santiago.v@dataproasesores.es](mailto:santiago.v@dataproasesores.es)**

**+34 609 024 024**