Agencia de Tecnología Legal

La (nueva) regulación de la Protección de Datos: de la LOPD al RGPD

COWORKING SPAIN CONFERENCE ~ 2018

COWORKINGSPAIN®

IMPACT HUB Madrid

Mayo, 2018

Carlos Galán es Doctor en Informática, Abogado especialista en Derecho de las Tecnologías de la Información, *Certified Information Security Manager* (CISM) por ISACA, Consultor/Formador Homologado de la EOI y Auditor Técnico de Certificación Productos, Procesos y Servicios de la Entidad Nacional de Acreditación (ENAC).

Autor de una decena de libros relacionados con las Tecnologías de la Información, su Derecho y sus aplicaciones, ha escrito asimismo una multiplicidad de artículos y comentarios en prensa y publicaciones especializadas. Ha desarrollado parte de su carrera profesional en el Grupo Telefónica, ocupando diversos cargos y participando en importantes proyectos nacionales e internacionales.

Ha sido Vocal Asesor y Director de la Oficina de Modernización del Ministerio del Interior, donde, entre otras actividades, diseñó en Plan de Modernización de los Cuerpos y Fuerzas de Seguridad del Estado y presidido la Comisión de Informática y Comunicaciones de la Seguridad de los Juegos Olímpicos de Barcelona '92.

Ha sido profesor de la Facultad de Informática de la Universidad Politécnica de Madrid, de la Escuela Técnica Superior de Ingenieros Industriales de la UNED, de la licenciatura de Administración y Dirección de Empresas de la Universidad Complutense de Madrid y del Instituto de Postgrado de la Universidad Pontificia de Comillas.

Ha sido Director General de la Agencia de Certificación Electrónica ACE (primera Autoridad de Certificación de España), Vicepresidente de la Asociación de Entidades de Confianza Digital AECODI, Director General de Desarrollo y Tecnología de la Fundación General de la Universidad de Málaga y Presidente del Comité de Nuevas Tecnologías de Hispajuris, la mayor red de despachos de abogados de España.

En el terreno académico, ha sido profesor de *Calidad, Seguridad y Protección de la Información*, de la Ingeniería de Informática de la Universidad Pontificia de Salamanca. Actualmente es miembro del Área de Derecho Administrativo de la Universidad Carlos III de Madrid, institución en la que imparte *Derecho de las TIC* en el Grado de Derecho de la Facultad de Ciencias Sociales y Jurídicas, y *Aspectos Legales de la Ingeniería Informática,* en el Máster de *Derecho de las Telecomunicaciones y Tecnologías de la Información,* actividades que compagina con la escritura de monografías y artículos y el dictado de conferencias y cursos donde es ponente habitual en las materias relativas al Derecho de las Tecnologías de la Información y las Comunicaciones, la Administración Electrónica, Firma Electrónica, Certificación Digital y Seguridad IT.

Ha sido asesor parlamentario en la redacción de la Ley 59/2003, de firma electrónica y, en la actualidad, es colaborador del Ministerio de Hacienda y Administraciones Públicas -dónde es miembro del Grupo de Expertos del Plan de Acción de Administración Electrónica 213-2015- y del Centro Criptológico Nacional –del Centro Nacional de Inteligencia-, en Administración Electrónica y Ciberseguridad, colaborando asimismo con varias organizaciones públicas y privadas. Es Presidente de la Agencia de Tecnología Legal, vicepresidente de la Comisión de Contratación Electrónica de la Asociación Nacional de Empresas de Internet, miembro del Observatorio Notarial para la Sociedad de la Información y miembro del Observatorio de la Mesa de la Justicia del Ilustre Colegio de Abogados de Madrid.

Agencia de Tecnología Legal

En, España, desde 1999, veníamos cumpliendo la Ley Orgánica 15/1999 LOPD (y, posteriormente, el RD 1720/2007 RDLOPD)…

(Por exigencia de la Directiva europea 95/46/CE)

Agencia de Tecnología Legal

Queda una semana para la plena aplicación del RGPD…

¿QUÉ NOS QUEDA POR HACER?

(← volver al índice)

Agencia de Tecnología Legal

¿QUÉ NOS QUEDA POR HACER?

1	**NUESTRA EMPRESA debe identificar con precisión las finalidades y la base jurídica de los tratamientos que se llevan a cabo.**	**Las finalidades o la base jurídica de los tratamientos son informaciones que deben proporcionarse a los interesados (arts. 13 y 14 RGPD) y recogerse en el registro de actividades de tratamiento.**

Legitimación de los tratamientos

El RGPD mantiene el principio recogido en la Directiva 95/46 de **que todo tratamiento de datos necesita apoyarse en una base que lo legitime**.

- **Consentimiento**.
- **Relación contractual.**
- Intereses vitales del interesado o de otras personas.
- **Obligación legal para el responsable.**
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

En ese sentido, el RGPD no implica cambios para los responsables del tratamiento de datos.

¿QUÉ NOS QUEDA POR HACER?

2	Cuando el tratamiento realizado por NUESTRA EMPRESA pudiera perseguir el cumplimiento de una tarea en interés público o el ejercicio de poder públicos, es necesario que el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma de rango legal.	

¿QUÉ NOS QUEDA POR HACER?

3	**Cuando la base jurídica de los tratamientos sea el consentimiento, tal consentimiento debe ser informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.**	**Los consentimientos conocidos como "tácitos", basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad.**

Ejemplo en una relación con un cliente:
Para EJECUTAR el contrato → **NO** se necesita recabar consentimiento del cliente.
Para remitirle una newsletter → **SÍ** se necesita.

El consentimiento

MANIFESTACIÓN DE VOLUNTAD

- **LIBRE**
- **ESPECÍFICA**
- **INFORMADA**
- **INEQUÍVOCA**

- una **DECLARACIÓN**
- una **CLARA ACCIÓN AFIRMATIVA**

- **No se admiten formas de consentimiento tácito o por omisión**, ya que se basan en la inacción.
- Hay situaciones en las que el consentimiento, además de inequívoco, ha de ser **EXPLÍCITO**:
  - Tratamiento de datos sensibles.
  - Adopción de decisiones automatizadas (perfilado).
  - Transferencias internacionales.

¿QUÉ NOS QUEDA POR HACER?

4	**Debe adecuarse la información que se ofrece a los interesados a las exigencias del RGPD (arts. 13 y 14), cuando NUESTRA EMPRESA recaba sus datos.**	**El RGPD obliga a ofrecer una información que es más amplia que la actualmente exigida por la LOPD. Obliga, además, a que esta información se proporcione de forma "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo".**

OBLIGACIONES:

Se establece una **LISTA EXHAUSTIVA de la información que debe proporcionarse** a los interesados (más amplia que la que actualmente contiene la LOPD) y que añade:

- **Base jurídica** del tratamiento
- Intención de realizar **transferencias internacionales**
- Datos del **Delegado de Protección de Datos** (si lo hubiere)
- Existencia de **decisiones automatizadas** (**Elaboración de perfiles)**

La información a los interesados deberá facilitarse **por escrito**, incluidos los **medios electrónicos** cuando sea apropiado.

¿QUÉ NOS QUEDA POR HACER?

5	**NUESTRA EMPRESA debe establecer mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos.**	**Estos mecanismos deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.**

PROCEDIMIENTO PARA EL EJERCICIO:

- Con carácter general, los RT deben **facilitar a los interesados el ejercicio de sus derechos**, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos. Se requiere que los responsables posibiliten la **presentación de solicitudes por medios electrónicos**, especialmente cuando el tratamiento se realiza por estos medios.
- El ejercicio de los derechos será **GRATUITO** para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas, el responsable podrá **cobrar un canon** que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para el responsable, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

¿QUÉ NOS QUEDA POR HACER?

6	**NUESTRA EMPRESA debe establecer procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD.**	**En algunos casos será preciso valorar la necesidad de que sean los Encargados del Tratamiento con los que NUESTRA EMPRESA haya contratado la prestación de determinados servicios los que colaboren en la atención a las solicitudes de los interesados.**

OBLIGACIONES:

- Articular procedimientos que **permitan que los interesados puedan acreditar que han ejercido sus derechos** por medios electrónicos (actualmente, en muchas ocasiones, no es viable).
- El responsable debe **demostrar el carácter infundado o excesivo** de las solicitudes que tengan un coste para el interesado.
- El responsable deberá **informar al interesado sobre las actuaciones derivadas de su petición** en el plazo de **un mes** (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes).
- Si el responsable decide **no atender una solicitud**, deberá informar de ello, motivando su negativa, dentro del plazo de **un mes** desde su presentación.

¿QUÉ NOS QUEDA POR HACER?

ANTES Debían facilitarse todos los datos de base del afectado, pero no copias o documentos (excepto en el caso de la historia clínica).

AHORA Se reconoce el **derecho a obtener una copia de los datos** personales objeto del tratamiento.

- Los responsables podrán atender a este derecho **facilitando el acceso remoto a un sistema seguro** que ofrezca al interesado un acceso directo a sus datos personales

¿QUÉ NOS QUEDA POR HACER?

7	**NUESTRA EMPRESA debe valorar si los encargados con los que haya contratado (o vaya a contratar) operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD.**	**El RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente a aquellos que estén en condiciones cumplir con el RGPD.**

¿QUÉ NOS QUEDA POR HACER?

ANTES:

- La Directiva 95/46 y en general las leyes nacionales se centran en la **actividad de los responsables**.

TRAS LA PLENA APLICACIÓN:

- El RGPD, por el contrario, contiene obligaciones expresamente dirigidas a **los encargados**.

En todo caso:

- **La responsabilidad última sobre el tratamiento sigue estando atribuida al RT**, que es quien determina la existencia del tratamiento y su finalidad.

¿QUÉ NOS QUEDA POR HACER?

- En determinadas materias **los ET tienen obligaciones propias** que establece el RGPD (no circunscritas al ámbito del contrato que los une al RT), y que **pueden ser supervisadas separadamente por las autoridades de protección de datos**. Por ejemplo:
  - 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 encargados pueden adherirse a **códigos de conducta** o certificarse en el marco de los **esquemas de certificación** previstos por el RGPD

¿QUÉ NOS QUEDA POR HACER?

8	**NUESTRA EMPRESA debe adecuar los contratos de encargo que actualmente tengan suscritos a las previsiones del RGPD.**	**El RGPD exige expresamente que tanto los contratos como los actos jurídicos deberán tener un contenido mínimo que excede del actualmente previsto por la normativa española de protección de datos.**

¿QUÉ NOS QUEDA POR HACER?

- Las relaciones entre el RT y el ET deben formalizarse en un **contrato que vincule al ET respecto al RT**.
- Se regula de forma minuciosa el **CONTENIDO MÍNIMO de los contratos** de encargo, debiendo preverse aspectos como:
  - **Objeto, duración, naturaleza y la finalidad** del tratamientos
  - **Tipo de datos personales y categorías** de interesados
  - Obligación del encargado de tratar los datos personales únicamente **siguiendo instrucciones documentadas** del RT
  - Condiciones para que el RT pueda dar su autorización previa, específica o general, a las **subcontrataciones**
  - **Asistencia al RT**, siempre que sea posible, en la atención al ejercicio de derechos de los interesados...

¿QUÉ NOS QUEDA POR HACER?

IMPORTANTE

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.

¿QUÉ NOS QUEDA POR HACER?

9	**Es necesario que NUESTRA EMPRESA desarrolle un <u>análisis del riesgo</u> para los derechos y libertades de los afectados de todos los tratamientos de datos que se acometan.**	

¿QUÉ NOS QUEDA POR HACER?

- **El RGPD condiciona la adopción de las medidas de responsabilidad activa al RIESGO que los tratamientos puedan suponer** para los derechos y libertades de los interesados. Se maneja el riesgo de dos maneras:
  - En algunos casos, prevé que **determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo** para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).
  - En otros casos, **las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve** (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

¿QUÉ NOS QUEDA POR HACER?

- Todos los RT deberán **realizar una valoración del riesgo de los tratamientos que realicen**, a fin de poder establecer **QUÉ** medidas deben aplicar y **CÓMO** deben hacerlo. El tipo de análisis variará en función de:

  - los tipos de tratamiento,
  - la naturaleza de los datos,
  - el número de interesados afectados,
  - la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

¿QUÉ NOS QUEDA POR HACER?

- **Preguntas para determinar el riesgo:**
  - ¿Se tratan datos sensibles?
  - ¿Se incluyen datos de una gran cantidad de personas?
  - ¿Incluye el tratamiento la elaboración de perfiles?
  - ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
  - ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
  - ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
  - ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas?

¿QUÉ NOS QUEDA POR HACER?

10	**NUESTRA EMPRESA debe establecer un Registro de Actividades de Tratamiento.**	**El RGPD establece un contenido mínimo de ese Registro, que deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.**

¿QUÉ NOS QUEDA POR HACER?

OBLIGACIONES:

- RTs y ETs deberán mantener un **registro de operaciones de tratamiento** en el que se contenga la información:
  - Nombre y datos de **contacto del RT y del Delegado de Protección de Datos**, si existiese.
  - **Finalidades** del tratamiento.
  - Descripción de **categorías de interesados y categorías de datos** personales tratados.
  - **Transferencias internacionales** de datos…
- Están **exentas** las **organizaciones que empleen a menos de 250 trabajadores**, salvo que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

¿QUÉ NOS QUEDA POR HACER?

11	**NUESTRA EMPRESA debe revisar las medidas de seguridad que se aplican a los tratamientos, a la luz de los resultados del análisis de riesgo de los mismos.**	**El RGPD deja sin efecto las previsiones del RD 1720/2007, en la medida en que exige que las medidas de seguridad se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes.**

¿QUÉ NOS QUEDA POR HACER?

ANTES:

- El RDLOPD (RD 1720/2007) determinaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento.
- Las medidas del RDLOPD estaban basadas casi exclusivamente en el tipo de datos que se trataban, con alguna matización relativa al contexto en que se llevaban a cabo los tratamientos.

TRAS LA PLENA APLICACIÓN:

- En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado **en función de los riesgos detectados en el análisis previo.**
- El RGPD pide que se tomen en consideración más variables.

¿QUÉ NOS QUEDA POR HACER?

- Las **medidas técnicas y organizativas** deberán establecerse teniendo en cuenta:
  - El coste de la técnica
  - Los costes de aplicación
  - La naturaleza, el alcance, el contexto y los fines del tratamiento
  - Los riesgos para los derechos y libertades

¿QUÉ NOS QUEDA POR HACER?

IMPORTANTE

El esquema de medidas de seguridad RDLOPD **no seguirá siendo válido de forma automática** tras la fecha de aplicación del RGPD.

En algunos casos **los responsables podrán seguir aplicando las mismas medidas que establece el Reglamento de la LOPD si los resultados del análisis de riesgos previo concluye que las medidas son realmente las más adecuadas** para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas.

¿QUÉ NOS QUEDA POR HACER?

12	**NUESTRA EMPRESA debe establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas.**	**Para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados.**

¿QUÉ NOS QUEDA POR HACER?

- El RGPD define las **violaciones de seguridad de los datos** (“*brechas de seguridad*”), incluyendo

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**.

[Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.]

¿QUÉ NOS QUEDA POR HACER?

- Cuando se produzca una violación de la seguridad de los datos, el responsable debe **notificarla a la autoridad de protección de datos competente**, salvo que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.
- La notificación de la quiebra a las autoridades debe producirse **sin dilación indebida** y, a ser posible, **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 adoptadas por el responsable para solventar la quiebra
  - si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados

¿QUÉ NOS QUEDA POR HACER?

- Los RT deben **documentar todas las violaciones de seguridad.**
- En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una **NOTIFICACIÓN DIRIGIDA A LOS INTERESADOS** (objetivo → permitir que puedan tomar medidas para protegerse de sus consecuencias. Debe realizarse sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas.)
- El RGPD añade a los contenidos de la notificación las **recomendaciones sobre las medidas que pueden tomar los interesados** para hacer frente a las consecuencias de la brecha.

¿QUÉ NOS QUEDA POR HACER?

- La notificación a los interesados **no será necesaria** cuando:
  - El RT hubiera tomado **medidas técnicas u organizativas apropiadas con anterioridad a la violación** de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el **cifrado**.
  - Cuando el RT haya tomado **con posterioridad** a la quiebra medidas técnicas que garanticen que **ya no hay posibilidad de que el alto riesgo se materialice**.
  - Cuando **la notificación suponga un esfuerzo desproporcionado**, debiendo en estos casos sustituirse por medidas alternativas como puede ser una **comunicación pública**.

¿QUÉ NOS QUEDA POR HACER?

13	**Necesidad de valorar si los tratamientos que se realizan en NUESTRA EMPRESA requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y de disponer de una metodología para llevarla a cabo.**	**El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo. También contempla un contenido mínimo de las Evaluaciones de Impacto.**

¿QUÉ NOS QUEDA POR HACER?

Lista indicativa de **supuestos que conllevan un ALTO RIESGO**:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar
- Tratamientos a gran escala de datos sensibles
- Observación sistemática a gran escala de una zona de acceso público

¿QUÉ NOS QUEDA POR HACER?

14	**Necesidad de valorar la designación de un Delegado de Protección de Datos (DPD/DPO).**	**El RGPD establece cuáles habrán de ser los criterios para la designación de los DPD/DPO, su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.**

¿QUÉ NOS QUEDA POR HACER?

- El RGPD establece la figura del **Delegado de Protección de Datos (DPD)**, que será **OBLIGATORIO** en:

  - **Autoridades y organismos públicos** (Se podrá designar un único delegado de protección de datos para varios organismos, teniendo en cuenta su estructura organizativa y tamaño).
  - RT o ET que tengan entre sus actividades principales las operaciones de tratamiento que requieran una **observación habitual y sistemática de interesados a gran escala**
  - RT o ET que tengan entre sus actividades principales el **tratamiento a gran escala de datos sensibles**

¿QUÉ NOS QUEDA POR HACER?

15	**Necesidad de adaptar los instrumentos de transferencia internacional de datos personales a las previsiones del RGPD.**	**El RGPD mantiene el modelo de transferencias internacionales ya existente, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que no requerirán de autorización previa de las autoridades de protección de datos.**

¿QUÉ NOS QUEDA POR HACER?

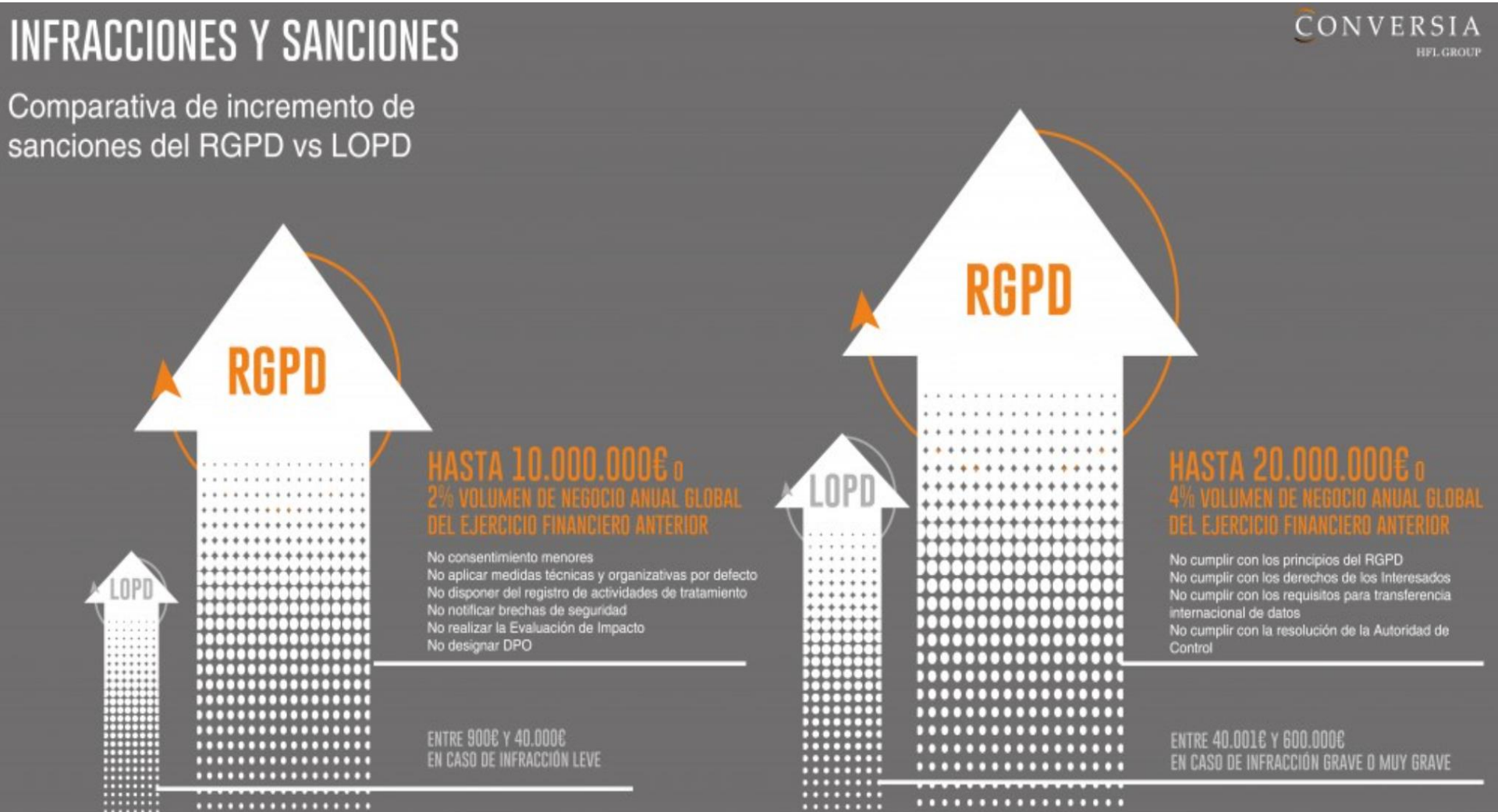
- El modelo de transferencias internacionales diseñado por el RGPD sigue los **mismos criterios que el establecido por la Directiva 95/46** y por las legislaciones nacionales de trasposición.
- Los datos **solo podrán ser comunicados fuera del EEE**:
  - A países, territorios o sectores específicos sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado
  - Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino
  - Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales

La parte mala…

Agencia de Tecnología Legal

¿QUÉ NOS QUEDA POR HACER?

Cada autoridad de control garantizará que la imposición de las **multas administrativas** sean en cada caso individual **efectivas, proporcionadas y disuasorias**.



Agencia de Tecnología Legal

La Protección de Datos y su adecuado tratamiento…

… depende de todos nosotros.

(← volver al índice)

Muchas GRACIAS

cgalan@atl.es

FORMACIÓN, CONSULTORÍA Y SOPORTE EN PROTECCIÓN DE DATOS, ADMINISTRACIÓN ELECTRÓNICA Y CIBERSEGURIDAD

CARLOS GALÁN