Solucyl
Consultores Tecnológicos, S.L.L.

Reglamento Europeo de Protección de Datos

José Daniel Fernández González

Doctor en Derecho – Graduado Social - Abogado

Wolters Kluwer | A3 Software

RGPD “NOTICIAS”


elEconomista.es
Tecnología
LAS HERRAMIENTAS FINAN
MÁS INNOVADORASDEL M
EN ECODIARIO.ES
El 'bombazo' del Real Madrid para la portería tiene nombre de viejo
Incumplir el nuevo reglamento de Protección de Datos estará sancionado con hasta 20 millones desde mayo
EUROPA PRESS 29/01/2018 - 17:18


cmm
CASTILLA-LA MANCHA MEDIA
CASTILLA-LA MANCHA ESPAÑA MUNDO DEPORTE CULTURA
Noticias / Mundo / El nuevo reglamento europeo para la protección de datos
El nuevo reglamento europeo para la protección de datos
28 Ene 2018 08:30
Este 28 de enero se celebra el Día Internacional de la Protección de Datos.

La conmemoración este domingo del Día Internacional de la Protección de Datos se produce en **plena cuenta atrás para que la nueva norma europea sea de obligado cumplimiento.** Prevé millonarias multas para las empresas que la incumplan y en España ya han avisado de que no habrá prórrogas en su aplicación.

El Reglamento General de Protección de Datos (RGPD) entró en vigor el 25 de mayo de 2016, pero **será a partir del 25 de mayo próximo cuando comience a aplicarse**, ya que este período de dos años ha servido para que empresas y organizaciones que tratan datos personales vayan preparándose y adaptándose.

Pero una vez que llegue el día D, **la norma se aplicará desde el “minuto uno”**, sin “régimen transitorio”, ni plazos, ni prórrogas, han advertido desde la Agencia Española de Protección de Datos (**AEPD**), organismo que velará en España por su cumplimiento.

“Todo el mundo ha tenido dos años para prepararse. A partir del 25 de mayo, se aplicarán para bien y para mal las obligaciones y los derechos del Reglamento”, afirmó esta semana la directora de la AEPD, Mar España, en un foro empresarial dedicado a la nueva norma.

“Soy consciente de la preocupación en el sector privado“, añadió la directora de la AEPD, que afirmó que su intención no es cargarse las empresas del país y expresó el “espíritu de ayuda y colaboración” de su organismo.


elEconomista.es
Empresas y finanzas
NUEVO
NISSAN QASHQAI
EN ECODIARIO.ES
El 'bombazo' del Real Madrid para la portería tiene nombre
Protección de Datos advierte sobre el nuevo Reglamento: se aplicará desde mayo y sin plazos


DIARIOJURÍDICO.com
GAVEL CAPITAL
PROFESIONALES JURÍDICOS LEGISLACIÓN Y JURISPRUDENCIA ARBITRAJE Y MEDIACIÓN
You are here: Home / Opinión / Novedades del nuevo Reglamento Europeo de Protección de Datos y diferencias con la LOPD
Novedades del nuevo Reglamento Europeo de Protección de Datos y diferencias con la LOPD
Publicado el 18 diciembre, 2017 por Redaccion
Con la mirada puesta en el **25 de mayo de 2018**, las empresas especializadas en LOPD seguimos dando respuesta a las preguntas que nos transmiten clientes, franquicias, colaboradores sobre si ¿Habrá muchos cambios con el nuevo Reglamento?, ¿Cuáles serán?, ¿Estoy obligado a adaptarme?, ¿La LOPD dejará de estar vigente?, ¿Por dónde empiezo?


Expansión
MERCADOS AHORRO EMPRESAS ECONOMÍA EXPANSIÓN&EMPLEO JURÍDICO TECNOLOGÍA OPINIÓN DIRECTIVOS
Jurídico Actualidad y Tendencias Fichajes Sentencias Opinión
CLÍNICA BAVIERA
Este mes 1ª Consulta GRATIS
ACTUALIDAD Y TENDENCIAS REGULACIÓN
¿Está preparada su empresa para el nuevo Reglamento de Protección de Datos?

Antecedentes (I)

Artículo 12 de la Declaración Universal de los Derechos del Hombre [París, Asamblea General de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948].

Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales (Roma, 14 de noviembre de 1950 –artículo 8– o el Pacto de los Derechos Civiles y Políticos –Nueva York, 19 de diciembre de 1966, artículos 17 y 19–).

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal ("LORTAD")

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

PIEDRA ANGULAR REGULACIÓN EUROPEA: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros.

Situación a partir de 25 de mayo de 2018

Solucyl Consultores Tecnológicos, S.L.L.

Wolters Kluwer | A3 Software

Ley Orgánica de Protección de Datos 15/1999 (LOPD)

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999

¿

Nueva Ley Orgánica de Protección de Datos
PENDIENTE APROBACIÓN

?

REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS (REPD)

Reglamento Europeo de Protección de Datos (REPD)

El Diario Oficial de la Unión Europea publicó el 4 de mayo de 2016 el ***«Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)»***.

El REPD propone un modelo de protección de datos basado en criterios como la responsabilidad activa, la flexibilidad, la importancia del contexto y la cooperación

Según el artículo 99 del REPD, éste entró en vigor a los veinte días de su publicación en el Diario Oficial de la UE, pero se establece en el apartado segundo de dicho precepto que será aplicable a partir del …

Principio de Transparencia

- *Antiguo principio del derecho de información del artículo 5 LOPD. El tratamiento de los datos de carácter personal debe realizarse de manera lícita, leal y transparente*.

- Derecho a estar informado de manera clara e inequívoca sobre el tratamiento que tiene al sujeto titular de los datos.

- Esto impone al responsable del fichero la obligación de facilitar la información que debe dar al sujeto titular tanto con carácter previo como en su caso, posterior si en un futuro se destinan a una nueva finalidad diferente por la cual se recabaron sus datos personales.

Principio de Limitación de la Finalidad

- Los datos serán recogidos con fines determinados, explícitos y legítimos. No serán tratados ulteriormente de manera incompatible con dichos fines (salvo que se informe de ello, previamente, y se obtenga el consentimiento del titular).

- El artículo 89.1 RGPD establece una excepción a este principio expresándose en los siguientes términos: *"el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos"* no se considera incompatible con los fines iniciales.

Principio de Minimización de Datos

- *Antiguo principio de calidad de los datos del artículo 4 LOPD*.

- El RGPD señala que los datos recabados para el tratamiento deben ser adecuados, pertinentes y limitados respecto a los fines para los que son tratados.

- Se está haciendo una clara alusión a la calidad del dato, a que sean proporcionales y no excesivos para el fin por el que van a ser tratados.

Otros Principios

Exactitud

Los datos personales recabados para el tratamiento deberán ser exactos, pero aquí no termina, sino que establece que si fuera necesario serán actualizados. Se deberán adoptar todas las medidas razonables para proceder de forma inmediata a la supresión o rectificación de aquellos datos que sean inexactos con respecto a los fines para los que se tratan.

Integridad y Confidencialidad

Se tendrá que garantizar que se establece una seguridad adecuada en función del tipo de dato personal en su tratamiento. Esto incluye aquellas medidas de seguridad organizativas y técnicas pertinentes que permitan protegerlos frente a todo tratamiento no autorizado o ilícito, su perdida, destrucción o daño accidental

Limitación Plazo de Conservación

Los datos serán conservados de tal manera que se permita la identificación de los interesados, únicamente, el tiempo que sea necesario para los fines del tratamiento.

Como excepción al plazo de conservación, los datos personales podrán ser mantenidos durante un tiempo superior siempre y cuando sean utilizados, exclusivamente, con fines de archivo en interés público, fines de investigación científica o histórica o estadística.

Responsabilidad Proactiva

Se pretende imponer al responsable del tratamiento la obligación de dar cabal cumplimiento de todos los principios mencionados y que sea capaz de demostrarlo, ASI: *Accountability* o de rendición de cuentas.

Condiciones para el Consentimiento

Solucyl Consultores Tecnológicos, S.L.L.

Wolters Kluwer | A3 Software

Situación Actual
Art. 7.2 y 7.3 LOPD

el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos, si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo».

- Cuando el tratamiento se base en el consentimiento del interesado, de nuevo, recae sobre el responsable del tratamiento la carga de la prueba de que aquel consintió el tratamiento de sus datos personales. En este sentido, la Agencia Española de Protección de Datos (en adelante, AEPD) destaca la importancia de revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.
- Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, su solicitud se presentará de tal forma que se distinga claramente de las demás cuestiones, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
- El interesado tendrá derecho a retirar su consentimiento en cualquier momento y ello no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello.
- Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Consentimiento de menores de edad

El artículo 8 y el Considerando (38) del RGPD se refieren al tratamiento de datos de menores y al consentimiento de los mismos. En estos preceptos se considera válido el consentimiento prestado por un menor de más de 16 años, existiendo la posibilidad para el legislador nacional de rebajar el umbral hasta los 13 años

En España es necesario contar con 14 años, si bien por debajo de esta edad se requiere el consentimiento de los padres o tutores.

Se fijan unas reglas especiales acerca de la **claridad de la información** que se debe mostrar a los menores, así como lo referido al derecho al borrado de la información. El responsable debe hacer "esfuerzos razonables para verificar la validez del consentimiento prestado por el menor.

Artículo 8 del anteproyecto de reforma de la LOPD: Artículo 8. Consentimiento de los menores de edad. *1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de trece años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. 2. El tratamiento de los datos de los menores de trece años sólo será lícito si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.*

Prohibición de Tratamiento

- ❑Los que revelen el origen étnico o racial.
- ❑Las opiniones políticas.
- ❑Las convicciones religiosas o filosóficas.
- ❑La afiliación sindical.
- ❑Los datos genéticos.
- ❑Los datos biométricos dirigidos a identificar de manera unívoca a una persona física.
- ❑Los relativos a la salud.
- ❑Los concernientes a la vida sexual o las orientaciones sexuales.

El RGPD considera que el tratamiento de fotografías no debe considerarse sistemáticamente comprendido en la norma general de los datos biométricos, sino únicamente cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física, como puede ser la tecnología de reconocimiento facial.

Excepciones a la Prohibición

- Cuando el interesado dio su consentimiento explícito, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición general no puede ser levantada por el interesado.
- Cuando el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una **fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical**, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.
- Cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.
- Cuando el tratamiento es necesario:
  - Para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho o de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.
  - Para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.
  - Para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
  - Por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
  - Para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario.
  - Por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.
  - Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Tratamiento de datos personales relativos a condenas e infracciones penales o medidas conexas de seguridad

¿Cuáles son?

Si bien la LOPD limita la inclusión de datos de carácter personal relativos a la comisión de infracciones penales a ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras, para el tratamiento de datos personales relativos a condenas, infracciones penales o medidas de seguridad conexas, el artículo 10 RGPD exige supervisión de las autoridades públicas o autorización del Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas

Derecho de Información

Art. 13 REPD

Datos Obtenidos del Interesado

- La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos, en su caso.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Los intereses legítimos del responsable o de un tercero, cuando el tratamiento se base en la necesidad para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- La intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, en su caso.
- La referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado, en el caso de las transferencias basadas en garantías adecuadas o normas corporativas vinculantes.

No obtenidos del Interesado

- La identidad y los datos de contacto del responsable y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos, en su caso.
- Los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento.
- Las categorías de datos personales de que se trate.
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- La referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado, en el caso de las transferencias basadas en garantías adecuadas o normas corporativas vinculantes

Derecho de acceso y de rectificación

Acceso

El artículo 15 REPD regula el **derecho de acceso** del interesado, estableciendo que tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, **derecho de acceso a los datos personales y a los fines del tratamiento**

Rectificación

El artículo 16 RGPD regula el **derecho de rectificación** del interesado, estableciendo que tendrá derecho a obtener la **rectificación de los datos personales inexactos** que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional

Derecho de Supresión (derecho al olvido)

*El artículo 17 RGPD regula el derecho de supresión del interesado, estableciendo que el interesado tendrá derecho a obtener la **supresión de los datos personales que le conciernan**, obligando al responsable del tratamiento a suprimir los datos personales cuando concurra alguna de las circunstancias siguientes:*

- ❑ Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- ❑ El interesado retire el consentimiento y este no se base en otro fundamento jurídico.
- ❑ El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.
- ❑ Los datos personales hayan sido tratados ilícitamente.
- ❑ Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- ❑ Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a menores de 16 años.

Recogido en la Sentencia del TJUE de 13 de mayo de 2014, supone que el interesado pueda solicitar el bloqueo de los resultados de los buscadores en Internet que se refieran a ellos y estas resulten obsoletas, incompletas, falsas o irrelevantes y no tengan un interés público.

Derecho a la limitación del tratamiento

El artículo 18 RGPD regula el derecho a la limitación del tratamiento, estableciendo que el interesado tendrá derecho a obtener del responsable del tratamiento dicha limitación cuando se cumpla alguna de las condiciones siguientes:

- ❑Que el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- ❑Que el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- ❑Que el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- ❑Que el interesado se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado

Derecho a la portabilidad de los datos

- Implica que el interesado puede solicitar a la entidad que esté tratando sus datos de forma automatizada, su recuperación en un formato que permita su traslado a otra entidad responsable, incluso de forma directa. Pensemos en los sistemas de computación en nube o *cloud computing*.
- Este derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el RGPD y, en particular, no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato,
- el 13 de diciembre de 2016, el Grupo de Trabajo del Artículo 29 (en adelante, GT29) ha publicado varias directrices (*WP 242/2016. Guidelines on the right to data portability* y *WP242 ANNEX–Frequently Asked Questions*. Grupo de Trabajo del Artículo 29. 13/12/2016) en las que se aclaran las condiciones en que se aplica este nuevo derecho, teniendo en cuenta la base jurídica del tratamiento de los datos (el consentimiento del interesado o en ejecución de un contrato) y el hecho de que este derecho se limita a los datos personales del interesado.

¿Cuándo sucederá esto?

Cuando el tratamiento esté basado en el consentimiento o sea necesario para la ejecución de un contrato.

Cuando el tratamiento se efectúe por medios automatizados

Tratamiento y acceso del público a documentos oficiales

El RGPD parte de que el acceso del público a documentos oficiales puede considerarse **de interés público**. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo.

- Ambos Derechos deben **conciliar** el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos.
- Por ello, el RGPD permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales.
- En resumen, con el objeto de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales, los contenidos en documentos oficiales en posesión de alguna autoridad pública u organismo público o una entidad privada para la realización de una misión en interés público podrán ser **comunicados por dicha autoridad, organismo o entidad** de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique.

Tratamiento del número nacional de identificación y tratamiento en el ámbito laboral

El RGPD confiere a los Estados miembros la potestad de **determinar**, adicionalmente, las **condiciones específicas** para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, dicho dato se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al Reglamento. Parece que la regulación de estas condiciones trae como consecuencia el auge de las actividades de suplantación de identidad y, con carácter particular, las realizadas por medios electrónicos.

En relación con el tratamiento de los datos personales **en el ámbito laboral**, una vez más, el RGPD confiere a los Estados miembros la posibilidad de establecer **normas más específicas** para garantizar la protección de los derechos y libertades:

- **Contratación de personal.**
- **Ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo.**
- **Gestión, planificación y organización del trabajo.**
- **Igualdad y diversidad en el lugar de trabajo.**
- **Salud y seguridad en el trabajo.**
- **Protección de los bienes de empleados o clientes.**
- **Ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo.**
- **Extinción de la relación laboral.**

La amplitud de materias que el Reglamento deja en manos de los Estados miembros para establecer normas más específicas nos puede hacer pensar que, lejos de tener como objetivo la unificación legislativa de los Estados miembros en materia de protección de datos de los trabajadores, da pie a que se produzcan grandes diferencias en este ámbito.

Tratamiento con fines de archivo en interés público, de investigación científica o histórica o fines estadísticos

- Como norma general, el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las **garantías adecuadas**, con arreglo al REPD, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales.
- Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su **consentimiento** para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica.
- Los interesados deben tener la oportunidad de dar su consentimiento solamente para **determinadas áreas de investigación o partes de proyectos de investigación**, en la medida en que lo permita la finalidad perseguida.
- El Derecho de la Unión o de los Estados miembros podrá establecer **excepciones** a los derechos acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos u oposición, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los siguientes fines: científicos o de interés público.

Otras Situaciones

Obligaciones de Secreto

- Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f) RGPD, en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una **obligación de secreto profesional o a otras obligaciones de secreto equivalentes**, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto.
- Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.
- Una vez más, cada Estado miembro tendrá que notificar a la Comisión las disposiciones legales adoptadas y cualquier modificación posterior de las mismas, como límite el 25 de mayo de 2018.

Normas sobre protección de datos de las iglesias y asociaciones religiosas

- Cuando en un Estado miembro, iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el RGPD.
- En ese caso, estarán sujetas al **control de una autoridad de control independiente**, que podrá ser específica, siempre que cumpla las normas establecidas en el Reglamento para las autoridades de control (capítulo VI).

El Responsable de Tratamiento

Es la persona que tiene la capacidad de determinar los fines y medios del tratamiento, siempre y cuando el Derecho de la Unión o los Estados miembros le otorgue dicha condición (art. 24 REPD)

- ❑ Protección de datos desde el diseño
- ❑ Protección de datos por defecto.
- ❑ Medidas de seguridad.
- ❑ Mantenimiento de un registro de tratamientos.
- ❑ Realización de evaluaciones de impacto sobre la protección de datos.
- ❑ Nombramiento de un delegado de protección de datos.
- ❑ Notificación de violaciones de la seguridad de los datos.
- ❑ Promoción de códigos de conducta y esquemas de certificación.

Medidas

Obligaciones del “RT”

- Aplicar medidas técnicas y organizativas apropiadas que permitan garantizar y demostrar que el tratamiento de los datos es conforme al Reglamento, identificándose que dichas medidas deben ser objeto de revisión y actualización cuando sea necesario. En este punto se produce una importante **novedad** puesto que **desaparece el elenco de medidas de seguridad al que estábamos acostumbrados** con el RLOPD. El RGPD se dota de una mayor flexibilidad y dinamismo con la previsión de que las medidas de seguridad que deben adoptarse deben ser las apropiadas. De modo que al no acotar las medidas de seguridad, tal y como están concebidas actualmente, le permite **adaptarse al rápido desarrollo tecnológico**.
- ***CRITICAS.*** La crítica positiva se corresponde con el que se haya evitado tasar un listado de medidas que pronto puedan ser consideradas obsoletas. Sin embargo, en muchas ocasiones se considera que algunas medidas de seguridad, en especial, medidas de tipo tecnológico, si bien pueden ser apropiadas no sean implantadas por el coste de su implantación, en atención al tamaño y recursos del responsable.
- La ventaja de la autorregulación reside en la importancia que a partir de ahora adquiere la **conservación de las evidencias necesarias**, en orden a demostrar que las medidas son objeto de revisión y actualización, no solo cuando sea necesario, sino para verificar su observancia e implantación. En cualquier caso, se debe de atender a los criterios interpretativos de las autoridades de control y al futuro que aguarda a la regulación prevista en el actual RLOPD, para poder adoptar medidas de seguridad que puedan considerarse apropiadas, en la medida que se desconoce qué técnica legislativa se utilizará para su derogación.

Corresponsables del tratamiento

Art. 26 REPD **regula la existencia de corresponsables** del tratamiento cuando dos o más responsables determinen los fines y los medios del tratamiento, exigiéndoles que doten de transparencia su conducta identificando contractualmente sus obligaciones en particular en lo referente a los aspectos…

- El ejercicio de los derechos del interesado.
- Sus respectivas cláusulas informativas que recojan la información que debe proporcionarse a los interesados cuando se obtengan los datos directamente del interesado o no, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos.
- Funciones y relaciones respectivas en relación con los interesados.
- Se confiere publicidad a los acuerdos mediante su puesta a disposición de los interesados de los que se pretenda obtener datos personales, debiendo informar de los aspectos esenciales de dicho acuerdo.
- El acuerdo podrá designar un punto de contacto para los interesados; sin embargo, no tiene relevancia su identificación puesto que los interesados podrán ejercer sus derechos frente a, y en contra de, cada uno de los responsables.

Representantes de responsables o encargados del tratamiento

- En el artículo 27 RGPD se establece la obligación para el responsable y el encargado de designar formalmente a un representante, siempre y cuando se aplique el REPD al tratamiento de datos efectuado por un responsable que no esté establecido en la Unión, es decir si nos encontramos en un lugar en que el Derecho de los Estados miembros sea de aplicación, en virtud del Derecho internacional público.
- El **requisito formal** que se atribuye a la designación es que la misma se **plasme por escrito**. Asimismo, y como es lógico, el requisito que se atribuye al representante para que ostente dicha condición es el de residir en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios o cuyo comportamiento esté siendo controlado.
- Sin embargo, la obligación de designar formalmente al representante no será aplicable en los casos en que el tratamiento de datos pueda ser considerado ocasional, siempre y cuando:

No incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9.1 RGPD

→ **O alternativamente** →

No incluyan el manejo de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento

A las autoridades u organismos públicos ← **O alternativamente** ←

Registro de las actividades de tratamiento

Artículo 30.1 RGPD establece la obligación de cada responsable y, en su caso, su representante de mantener un **registro de las actividades de tratamiento**, de manera muy similar a la obligación actual de declaración de ficheros a la AEPD, pero dicha obligación desaparece para convertirse en un registro de carácter interno que, formalmente debe constar por escrito y también en formato electrónico. Este registro estará a disposición de la autoridad de control en el caso de que lo solicite. La información del registro de actividades del responsable deberá contener la siguiente información:

- ❑ **Nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del delegado de protección de datos.**
- ❑ **Fines del tratamiento.**
- ❑ **Descripción de las categorías de interesados.**
- ❑ **Descripción de las categorías de datos personales.**
- ❑ **Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.**
- ❑ **Transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias puntuales (se hace referencia a las transferencias identificadas en el artículo 49.1.2º párrafo RGPD), la documentación de garantías adecuadas.**
- ❑ **Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.**
- ❑ **Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.**

Protección de datos desde el diseño

- El artículo 25.1 REPD establece la **obligatoriedad** de aplicar el principio de protección de datos desde el diseño y tener en consideración la privacidad de los interesados respecto de los cuales haya obtenido datos, durante toda la vida del dato, es decir desde su obtención hasta su efectiva destrucción, pasando por todas las fases de su tratamiento.
- Se trata de una de las obligaciones de **carácter proactivo** y no reactivo del responsable del tratamiento, obligando a establecer controles que revisen periódicamente el cumplimiento de las previsiones del REPD, con la finalidad de corregir las no conformidades que se detecten o mejorar aquellos aspectos que sean susceptibles de mejora, con el fin último de proteger los derechos de los interesados.

El RGPD prevé, de manera específica, aquellos momentos en los que debe ser tenido en cuenta este principio, siempre y cuando se pretenda desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, siendo los siguientes:
•A priori, en el **momento de determinar los medios de tratamiento**.
•**Durante** el propio tratamiento.

Momentos a Tener en cuenta

Factores

También se prevé que la obligación de las medidas, o el modo en que se apliquen, **dependerá de los siguientes factores**:
- El estado de la técnica.
- El coste de la aplicación.
- La naturaleza, ámbito, contexto y fines del tratamiento.
- Los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

Da Valor añadido a un modelo de negocio basado en el respeto de la privacidad de los individuos.
ventajas desde el **punto de vista del usuario**:
- Percepción de que se otorga una especial protección a sus datos.
- Incremento de su confianza en el mercado global.
- Debe ser considerado como beneficioso para el buen desarrollo de un proyecto y no como una pérdida de oportunidad, pues ser capaz de conocer los riesgos permite implementar los medios necesarios para mitigarlos.

Ventajas

Protección de datos por defecto (I)

El artículo 25.2 RGPD prevé la **obligatoriedad** del responsable de **aplicar las medidas técnicas y organizativas apropiadas** con la finalidad de que, por defecto, solo serán objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. En este sentido, este principio se encuentra íntimamente relacionado con el principio de **calidad de los datos**, de manera que debe olvidarse del concepto "cuanta más información tenga, mejor", sino que debemos valorar si cada uno de los datos que se van a solicitar a los interesados son necesarios o no. Los responsables, en la configuración del principio "por defecto" deberán tener en cuenta los siguientes parámetros:

- ❑La cantidad de datos personales recogidos.
- ❑La extensión de su tratamiento.
- ❑Su plazo de conservación.
- ❑Su accesibilidad.

Herramienta "FACILITA"

http://www.servicios.agpd.es/ENQUEST4/view/form/MDAwMDAwMDAwMDAwMDEzMDM2MTcxNTIyNDk5MzQzODk4?updated=true

Protección de datos por defecto (II)

¿Qué Implica?

Privacidad por defecto, de manera muy simplificada, implica que siempre debe aplicarse la **configuración de privacidad más estricta** con carácter automático cuando un cliente adquiere un nuevo producto o servicio. En otras palabras, el usuario no debe cambiar de manera manual las opciones que le permitan restringir su privacidad cuando solicite un servicio. El principio se considera fundamental para garantizar la privacidad en las plataformas de redes sociales y, con carácter particular, entendemos que se ha pretendido proteger a los usuarios más jóvenes o menos habituados a trabajar con nuevas tecnologías.

Ejemplo

Si deseamos registrarnos en una red social en la que se puede compartir información personal, acontecimientos de la vida u otro contenido que consideremos relevante y el registro para poder publicar nuestro perfil solo exige nuestro nombre y dirección de correo electrónico; sin embargo, en nuestro perfil también se publica de manera automática la edad, la ubicación, etc., se hacen públicas. Es decir, disponible al público en general y no solo a los contactos que previamente hemos aprobado o solicitado. Este caso, sería una clara infracción del principio por defecto, puesto que se proporciona, por defecto, más información de la estrictamente necesaria para poder registrar nuestro perfil.

El encargado del tratamiento

Se corresponde con la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (art. 28 REPD)

Elección

La elección de cada encargado adquiere especial relevancia para los responsables, pues pueden ser elegidos únicamente si ofrecen garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, en orden a que el tratamiento que efectúe sea conforme al Reglamento y garantice la protección de los derechos del interesado

El RGPD será de aplicación no solo a encargados establecidos en la Unión Europea, sino que extiende a encargados no establecidos en la Unión, siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

el artículo 27 RGPD establece la obligación del encargado de nombrar un representante siempre y cuando se aplique el RGPD al tratamiento de datos efectuado por un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación, en virtud del Derecho Internacional público

Regulación contractual de su relación con el responsable

- el RGPD continúa exigiendo que la relación entre el responsable y encargado se regule en un **contrato u otro acto jurídico análogo** conforme al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable en el que se identifique el objeto, duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.
- El requisito formal del contrato exige que el mismo se plasme por escrito, incluso en formato electrónico. Asimismo sin perjuicio, del contrato que establezcan responsable y encargado, su contenido, podrá reproducir o incluir algunas de las cláusulas contractuales tipo que se desarrollen por parte de las autoridades de control, en aplicación del mecanismo de coherencia.

*Tratará los datos personales **únicamente siguiendo instrucciones documentadas del responsable**, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. Esta prohibición de no informar al responsable se ha previsto para aquellos casos en que dicho encargado venga, por ejemplo, a informar de actividades del responsable a organismos que, de no hacerlo, incurriría en responsabilidad.*

Obligaciones

Obligaciones del Contrato

- Garantizará que su personal disponga de un **compromiso de confidencialidad** o esté sujeto a una obligación de confidencialidad de naturaleza estatutaria (por ejemplo, médicos, abogados, que ya disponen de un código deontológico profesional). Esta última previsión supone una novedad en la medida que equipara el deber de secreto del personal con el deber de secreto profesional.
- Tomará todas las **medidas de seguridad** técnicas y organizativas apropiadas y necesarias.
- **Regulación de la subcontratación**: autorización previa, información de cambios en la identidad de los subcontratados con la finalidad de que el responsable pueda oponerse al mismo, firma de un contrato entre encargado y subencargado.
- Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de **medidas técnicas y organizativas apropiadas**, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.
- Ayudará al responsable a **garantizar** el cumplimiento de las obligaciones relacionadas con la seguridad del tratamiento; la notificación de una violación de los datos a una autoridad de control y, en su caso, al interesado; la evaluación de impacto y la consulta previa, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.
- A elección del responsable, **suprimirá o devolverá todos los datos personales** una vez **finalice** la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros. En este punto, viene a matizarse la discrecionalidad del responsable de poder optar por la devolución o la supresión de los datos personales.
- Pondrá a **disposición del responsable** toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
- Informará al responsable si detecta que entre la información que debe proporcionar al responsable, en su opinión, una instrucción **infringe** el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

Subcontratación de servicios

El encargado puede subcontratar sus servicios, siempre y cuando disponga de la autorización previa por escrito del responsable.

- Esta autorización, que podrá ser general o específica, formará parte del contrato o acuerdo que regule la relación entre ambos.
- La autorización general se ha previsto para aquellos casos en los que el encargado no pueda identificar a los subcontratistas, puesto que se otorga al responsable un poder de control sobre la incorporación de nuevos encargados o la sustitución de otros, de tal manera que se le concede la oportunidad de que pueda oponerse a dichos cambios.
- En cualquier caso, el primer encargado responde frente al responsable respecto al cumplimiento de las obligaciones del subcontratista

La violación de la seguridad

Estaremos ante una violación de la seguridad cuando se produzca un evento que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, cualquiera que sea la forma de su tratamiento o la comunicación o acceso no autorizados a dichos datos

Daños y Perjuicios

Son innumerables los daños y perjuicios que para los interesados pueden derivarse de una violación de la seguridad, tales como la pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras o cualquier otro perjuicio económico o social significativo para la persona. De modo que, la notificación de la violación de la seguridad de los datos a la autoridad de control y, en su caso, al interesado, se configura como clave en orden a que se adopten las cautelas precisas para minimizar los riesgos de este tipo de eventos.

La comunicación de las violaciones de seguridad, que comúnmente vienen también siendo denominadas como "brechas de seguridad", no se considera una novedad en el ordenamiento jurídico puesto que la Directiva 2002/58/CE y el Reglamento (UE) nº 611/2013 introdujeron y desarrollaron dicha obligación en el ámbito del tratamiento de datos personales en el sector de los prestadores de servicios de comunicaciones electrónicas

Directiva 2002/58/CE y el Reglamento (UE) nº 611/2013

Dictamen 03/2014

El Dictamen 03/2014 sobre la notificación de violación de datos personales del grupo de trabajo del artículo 29 analizó las directrices que ayudarían a los responsables a decidir si debían notificar a las personas afectadas la "violación de datos personales" en caso de que se materializasen, teniendo en consideración no solo la obligación de la Directiva 2002/58/CE que incumbía a los proveedores de comunicaciones electrónicas, sino que también tuvo en cuenta el contexto de la propuesta del, entonces futuro RGPD, incluyendo lo que se consideraban como buenas prácticas para todos los responsables del tratamiento con ejemplos de múltiples sectores.

Notificación a la autoridad de control

El artículo 33 RGPD establece el momento en el cual se debe proceder a la notificación de la violación de seguridad a la autoridad de control competente:

- **Sin dilación indebida**. En la práctica, se producirá cuando se tenga preparado el documento de notificación y antes de las 72 horas.
- **Si es posible, en el plazo máximo de 72 desde su conocimiento**, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.
- **Si transcurren 72 horas, la notificación debe identificar los motivos que han llevado al responsable a la necesidad de que haya agotado dicho plazo**. En este punto será clave identificar correctamente y mantener las evidencias necesarias del momento en el que se haya tenido constancia de la violación

https://sedeagpd.gob.es

Contenido de la notificación

Contenido

- ❑ Describir la naturaleza de la violación y, siempre que sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- ❑ El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- ❑ Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- ❑ Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

El REPD permite que la información de la notificación **no se proporcione de manera simultánea**, admitiéndose que inicialmente se pueda facilitar de manera incompleta; si bien señala que se facilitará de manera **gradual** sin dilación indebida.
En cualquier caso, entendemos que el momento de la notificación, junto con la rapidez en la que se notifique la violación, serán aspectos que se consideren fundamentales en orden a **demostrar la diligencia** debida en la cumplimentación de este trámite.
Se desconocen actualmente las consecuencias directas que tendrá la notificación por parte de la autoridad de control. Sin embargo, no debe dejarse de lado que deberá **atenderse a su naturaleza y las circunstancias en las que se haya producido**, para que la autoridad de control sancione la actividad del responsable. Sin embargo sí se prevé en el considerando (87) que dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el RGPD.

Notificación al interesado

El artículo 34 RGPD establece la obligación de comunicar una violación de los datos al interesado cuando sea probable que entrañe un alto riesgo para los derechos y libertades de las personas físicas. El RGPD no establece ningún plazo para su notificación, limitándose a identificar que la comunicará sin dilación indebida. Asimismo señala que la forma en que debe proporcionarse la información debe realizarse en un lenguaje claro y sencillo y tendrá carácter gratuito.

Contenido Minimo

- ❑ El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- ❑ Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- ❑ Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

No es Necesario

- ❑ Si se habían adoptado medidas de protección técnicas y organizativas apropiadas como que los datos objeto de violación estuviesen cifrados.
- ❑ Adopción de medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado
- ❑ Cuando suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. En este punto, pueden tomarse como ejemplos, la publicación de la noticia en medios de comunicación o redes sociales. Sin embargo, suelen llevar aparejado un daño en la imagen corporativa que puede ser incluso superior que el de su sanción económica.

siempre quedará bajo criterio de la autoridad de control que pueda exigir al responsable que se lleve a cabo la notificación al interesado o apreciar que se cumple con alguna de las condiciones identificadas anteriormente para que no lo haga.
Por último, el artículo 23 REPD identifica las limitaciones, donde se establece la reserva de que el Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en relación a la notificación de una violación al interesado

La Evaluación de Impacto

- La gestión de riesgos en el ámbito de protección de datos se configura como una **herramienta novedosa** regulada en el artículo 35 REPD.
- En nuestro país, la Evaluación de Impacto en la Protección de los Datos Personales (EIPD) se introdujo por la AEPD en el año 2014, facilitando un marco de referencia flexible y de buenas prácticas a seguir mediante la publicación de la "Guía para una Evaluación de Impacto en la Protección de Datos Personales". La guía, en su introducción, señalaba que se quería promover el compromiso responsable de las entidades que trataban datos dando un paso más allá del mero cumplimiento normativo.
- La evaluación de impacto, más conocida como PIA, por sus siglas en inglés (*Privacy Impact Assessments*), se ha venido desarrollando fundamentalmente en países anglosajones, donde ya existían metodologías consolidadas para su realización.
- El enfoque de la evaluación de riesgos que lleva a cabo el RGPD se configura como un **enfoque global** de la gestión de riesgos, dirigido a manejar la incertidumbre relativa a la materialización de una amenaza, a través de la propia evaluación, en orden a establecer las oportunas estrategias de desarrollo para manejarlo y mitigarlo

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

¿Cuándo se lleva a cabo EI?

- La evaluación viene exigida cuando que exista una probabilidad de que un tipo de tratamiento, y de manera particular si se utilizan nuevas tecnologías, entrañe un **alto riesgo** para los derechos y libertades de las personas físicas. La probabilidad de que el tipo de tratamiento entrañe riesgos debe valorarse atendiendo a los siguientes criterios: su naturaleza, su alcance y el contexto o los fines del tipo de tratamiento.
- El RGPD añade la posibilidad de que una única evaluación pueda abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. Esta circunstancia, según el considerando (92), se ha previsto en el RGPD atendiendo a circunstancias en las que pueda ser razonable y económico que una evaluación abarque más de un único proyecto. Podemos mencionar, como ejemplo, el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyectan introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.
- En la práctica, entendemos que quedará relegado a mecanismos de cooperación interadministrativa, puesto que será difícil que responsables del ámbito privado se pongan de acuerdo para llevar a cabo evaluaciones de proyectos que aún no han salido a la luz y de los que se mantiene un absoluto sigilo en términos empresariales.
- El REPD introduce en la regulación de la evaluación una de las funciones del delegado de protección de datos, obligando al responsable a recabar su asesoramiento al realizar la evaluación de impacto, siempre y cuando dicha figura exista dentro de la organización.

Aspectos Principales CC

- El artículo 40 RGPD señala que aquellas empresas que lleven a cabo algún tratamiento de datos de carácter personal podrán adherirse a **un código de conducta ya existente, elaborar uno o modificar** otra ya existente, con el fin de favorecer la aplicación del REPD.
- La autoridad de control competente (AEPD) tendrá que aprobar los códigos aplicables y, posteriormente, proceder a registrarlos y publicarlos

1. Adherirse a uno de ellos o a participar o colaborar en la redacción de uno nuevo, pero una vez adherido a uno de ellos, está obligado al cumplimiento de las pautas marcadas por él.
2. De esta manera, una empresa de un determinado sector que se adhiera a un código de conducta elaborado para ese colectivo gozará, a priori, de una imagen de garantía y seguridad de cara a los interesados y de la propia autoridad de control.
3. El objetivo de los códigos de conducta consiste en establecer una alternativa a través de la cual facilitar el cumplimiento del RGPD en función de las peculiaridades estándar de cada sector.
4. Es decir, son un conjunto de pautas y normas de buen hacer, de buena praxis y conducta, adoptadas como modelos a seguir por empresas que pertenezcan a un mismo sector, respetando y favoreciendo el cumplimiento del contenido del RGPD.

El responsable del tratamiento no está obligado a:

Procedimiento de elaboración, modificación o ampliación CC

Para contribuir al correcto cumplimiento del RGPD, los Estados miembros, autoridades de control, el Comité y la Comisión promoverán la elaboración de los códigos de conducta. Durante su elaboración deberán tener en consideración las especificidades propias y necesidades de los diferentes sectores de tratamiento

Si el proyecto del código de conducta, modificación o ampliación es aprobado y no se refiere a actividades de tratamiento en otros Estados miembros, la autoridad de control **lo registrará y publicará**.

NO hay actividades de tratamiento en otros Estados miembros

SI hay actividades de tratamiento en otros Estados miembros

- Cuando el proyecto del código de conducta guarde relación con actividades de tratamiento en otros Estados miembros, la autoridad de control que sea competente (es decir, aquella que pueda desempeñar sus funciones asignadas y ejercer sus poderes en el territorio de su Estados miembros) **lo presentará antes de aprobarlo, modificarlo o ampliarlo al Comité**, a través de un procedimiento de cooperación entre las autoridades de control y la Comisión. Se trata de un procedimiento basado en un mecanismo de coherencia cuyo objeto es contribuir a una aplicación coherente del RGPD. De este modo, el Comité dictaminará si el proyecto, modificación o ampliación es conforme al RGPD y, si lo es, presentará su dictamen a la Comisión.
- La Comisión tiene competencia para decidir si el código de conducta, modificación o ampliación, aprobados y presentados conforme al procedimiento establecido en el RGPD, tiene o no validez general dentro de la Unión. A continuación, la Comisión dará publicidad adecuada de validez general a los códigos aprobados.
- Posteriormente, el Comité archivará en un registro cada uno de los códigos de conducta, modificaciones o ampliaciones que se aprueben, estando a disposición pública.

Supervisión de CC

*El código de conducta estará supervisado por la **autoridad de control competente**, que velará por el cumplimiento de las disposiciones e instrucciones que contenga por parte de los responsables o encargados del tratamiento que se adhieran. Asimismo, se establece la posibilidad de que un organismo ajeno a la autoridad de control posea la facultad de supervisión del código de conducta, siempre y cuando tenga un nivel adecuado de pericia en relación con el objeto del código y, previamente, sea acreditado por la autoridad de control competente.*

Sin embargo, no es tarea fácil que un organismo ajeno a la autoridad de control sea supervisor de un código de conducta, pues además de necesitar demostrar su nivel de pericia con el objeto del código es necesario que cumpla una serie de requisitos (establecidos en el artículo 41 RGPD) para poder ser acreditado al efecto por la autoridad de control

1. Demostrar su nivel de pericia e independencia respecto al código de conducta.
2. Establecer procedimientos a través de los cuales sea capaz de supervisar el cumplimiento del código, evaluar de forma periódica su aplicación, así como valorar la idoneidad de los responsables o encargados correspondientes para aplicarlo.
3. Tener un conjunto de procedimientos y estructuras transparentes para el público e interesados, y que sean pertinentes para poder gestionar las reclamaciones relativas a infracciones del código.
4. Demostrar a la autoridad de control competente que sus funciones nos dan lugar a una situación de conflicto de intereses

Requisitos

La autoridad de control competente tiene la facultad y poder para revocar la acreditación otorgada a un organismo si no cumple con los requisitos, si deja de cumplirlos o si la actuación del organismo infringe el RGPD

Mecanismos de certificación, sellos y marcas

El artículo 42 RGPD impone la obligación a los Estados miembros, las autoridades de control, el Comité y la Comisión de **promover**, dentro del ámbito de la Unión, la creación de mecanismos de certificación, sellos y marcas de protección de datos que tienen como objetivo demostrar el cumplimiento del RGPD en las operaciones realizadas por responsables o encargados del tratamiento.

Situaciones

1. Se podrán adherir a los mecanismos de certificación, sello o marcas de protección de datos, los responsables o encargados del tratamiento sujetos al cumplimiento del RGPD (artículo 3 RGPD - ámbito territorial).
2. Asimismo, se podrán constituir mecanismos de certificación, sellos o marcas con el fin de que tanto por parte de responsables o encargados del tratamiento no sujetos al RGPD, como en el marco de transferencias de datos a terceros países u organizaciones internacionales, puedan demostrar garantías adecuadas por estos medios. De este modo, estos responsables o encargados no sujetos deberán asumir compromisos vinculantes y exigibles, por vía contractual o a través de instrumentos jurídicos vinculantes, para aplicar las garantías adecuadas, tales como las relativas a los derechos de los interesados

Caracteristicas

1. Se atenderá a los criterios establecidos por Dicha **autoridad de control** o el **Comité** mediante el mecanismo de coherencia. Es decir, a través del procedimiento de cooperación establecido en el artículo 63 REPD.
2. El Comité archivará los mecanismos de certificación, sellos o marcas de protección en un registro que estará a disposición pública. En todo caso, la adhesión será voluntaria, estando disponible a través de un proceso trasparente. los responsables o encargados del tratamiento de datos que se adhieran a un mecanismo de certificación deberán facilitar toda la información y el acceso a las actividades de tratamiento que sean necesarias para llevar a cabo el procedimiento de certificación a la autoridad de control competente o al organismo de certificación.
3. La duración de la certificación expedida a un responsable o encargado será por un periodo de tres años. Será renovable teniendo en cuenta los mismos criterios, siempre y cuando se continúe cumpliendo con los requisitos pertinentes. La autoridad de control competente o el organismo de certificación podrán retirar la certificación cuando no se cumplan los requisitos de la misma o se hayan dejado de cumplir.

El organismo de certificación

Los Estados miembros garantizarán que los organismos de certificación sean acreditados por una de las siguientes entidades o, en su caso, por ambas al mismo tiempo

- La autoridad de control competente.
- El organismo nacional de acreditación designado conforme al Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo

La acreditación de los organismos de certificación se llevará a cabo en atención a los criterios establecidos aprobados por una de las siguientes entidades

- La autoridad de control.
- El Comité de conformidad

Sin perjuicio de las funciones y poderes que el REPD otorga a las autoridades de control en sus artículos 57 y 58, se confiere poder para expedir y renovar certificaciones a los organismos de certificación siempre que tengan un **adecuado nivel de pericia en protección de datos**.
Previamente, deberán haber informado a la autoridad de control, con el objeto de que esta pueda, en su caso, ejercer los poderes correctivos que le otorga el artículo 58 RGPD y, en particular, el poder para retirar una certificación, así como el de ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para obtener la certificación.

Tratamiento transfronterizo y transferencia internacional de datos

Actualmente, debido a la implementación de nuevas tecnologías en la sociedad y, en concreto en el ámbito empresarial, se ha visto **incrementado** exponencialmente el volumen de intercambio de información y de datos personales, que cada día adquieren más valor

- Este escenario da lugar a nuevos retos y amenazas que ya están afectando a la protección de los datos personales. Tal y como expone el RGPD, en aquellos casos en los que se transfieren datos de la Unión hacia responsables, encargados u otros destinatarios ubicados en un tercer país fuera de la Unión o a organizaciones internacionales, se debe velar por garantizar **que se mantenga el nivel de protección de los datos** de las personas físicas garantizado en la Unión.

- Asimismo, esto se tiene que extrapolar en aquellas transferencias que se realicen, posteriormente, en el mismo u otro tercer país fuera de la Unión u Organización Internacional

Se entiende por tratamiento transfronterizo todo tratamiento de datos de carácter personal realizado en el ámbito de actividades de establecimientos situados en más de un Estado miembro de un responsable o de un encargado del tratamiento en la Unión Europea, si el responsable o encargado se encuentra ubicado en más de un Estado miembro.
Asimismo, también se entiende por tratamiento transfronterizo, el tratamiento de datos realizado en el ámbito de las actividades de un Estado miembro de un responsable o encargado de la Unión, pero que puede las afectar sustancialmente a interesados en más de un Estado miembro

El RGPD dedica su capítulo V a las transferencias de datos personales a terceros países u organizaciones. En concreto, el artículo 44 REPD establece como principio general que, solo se llevarán a cabo transferencias de datos que tengan por objeto un tratamiento o vayan a tenerlo, tras la transferencia, a un tercer país fuera de la Unión u Organización Internacional, si el responsable y encargado del tratamiento cumplen:

- Lo dispuesto en el RGPD y en concreto su capítulo V.
- Extrapolar lo dispuesto en RGPD respecto aquellas transferencias que se realicen posteriormente en el mismo u otro tercer país fuera de la Unión u Organización Internacional.

¿Cómo se realizan transferencias internacionales?

- Mediante acto ejecutivo de la Comisión que confirme que se establece un nivel de protección adecuado.
- Cuando se establezcan garantías adecuadas para compensar la ausencia de decisión de adecuación al RGPD por parte de la Comisión, tales como normas corporativas vinculantes o *Binding Corporate Rules* (BCR).
- Si estamos ante alguna de las excepciones que se aplican en situaciones específicas.

Se podrá realizar una transferencia de datos a un tercer país u Organización Internacional, cuando la Comisión decida que garantizan un nivel de protección adecuado

1. Un tercer país.
2. Un territorio.
3. Uno o varios sectores específicos del mismo.
4. La Organización Internacional.
5. Asimismo, dicha transferencia de datos no requerirá ninguna autorización específica para llevarla a cabo. Sin embargo, la Comisión podrá revocar esta decisión de valoración, con preaviso y mediante declaración motivada al tercer país u Organización Internacional.

Ejemplo

Safe Harbor Agreement **o Acuerdo de Puerto Seguro. Durante años parecía ser un mecanismo fiable que garantizaba la transferencia internacional de datos de carácter personal desde la Unión a EE. UU. No obstante, tras ser estudiado y reanalizado a posteriori se pudo corroborar que debido a normativa nacional de EE. UU. y, en concreto, la relativa a la defensa nacional, se estaban produciendo vulneraciones en los derechos de los ciudadanos europeos en materia de privacidad y protección de datos. Por ello, en octubre de 2015 el Tribunal de Justicia de la Unión anuló el Acuerdo de Puerto Seguro, declarando que EE. UU. no garantizaba un nivel adecuado de protección**

Evaluación del tercer País

Será la Comisión la que podrá decidir si se ofrece o no un nivel de protección de datos adecuado y con efectos en toda la Unión. En la evaluación del tercer país, territorio o sector específico del mismo, se tendrá **en consideración**:

- Si el tercer país respeta el Estado de Derecho, valores fundamentales en los que se basa la Unión, el acceso a la justicia, normas y criterios internacionales en materia de derechos humanos, etc. De esta manera, se contribuye a que encontremos en toda la Unión seguridad y uniformidad jurídica respecto a la valoración del nivel de protección que ofrece el tercer país u Organización Internacional.
- La existencia y correcto funcionamiento de autoridades de control independientes para garantizar que se cumplen con las normas de protección de datos, tanto en terceros países, como en las que se encuentre sujeta una Organización Internacional.
- Las obligaciones que figuren en acuerdos o instrumentos jurídicamente vinculantes y los compromisos internacionales que sean asumidos por el tercer país u Organización Internacional.

Nivel de Protección

- El tercer país, para que se considere que ofrece garantías, debe asegurar un **nivel adecuado de protección** equivalente a lo estipulado en la Unión. Asimismo, el tercer país debe garantizar que haya un control independiente de la protección de datos, así como establecer mecanismos de cooperación con las autoridades de control de los Estados miembros, reconocer a los interesados sus derechos exigibles y contar con acciones administrativas y judiciales efectivas.
- Posteriormente, tras la evaluación del nivel de protección, será la Comisión la que decidirá mediante un acto de ejecución si un tercer país, territorio, uno o varios sectores específicos o una Organización Internacional garantizan un nivel de protección adecuado, tal y como establece el RGPD. El acto de ejecución que da validez a la realización de transferencias internacionales tendrá, al menos cada cuatro años, una revisión para garantizar que se sigue cumpliendo y manteniendo un nivel adecuado de protección.
- Por el contrario, si durante la supervisión de la Comisión resulta una valoración negativa, es decir, deja de garantizar el nivel óptimo de protección, la Comisión deberá derogar, modificar o suspender la decisión que se adoptó en su momento, mediante actos de ejecución. A continuación, comenzarán rondas de consultas con el tercer país u Organización Internacional con el fin de intentar subsanar esta situación.

Mediante el establecimiento de garantías adecuadas

Sin necesidad de autorización expresa de una autoridad de control competente

- Normas corporativas vinculantes o *Binding Corporate Rules (BCR).*
- Instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
- Cláusulas tipo de protección de datos adoptadas por la Comisión o la autoridad de control.
- Códigos de Conducta o mecanismos de certificación, junto con el establecimiento de compromisos vinculantes y exigibles al responsable o encargado del tratamiento en un tercer país.

Con necesidad de autorización expresa de una autoridad de control competente

- Cláusulas contractuales debidamente autorizadas por una autoridad de control, entre el responsable o el encargado, con el responsable, encargado o destinatario de los datos en el tercer país u Organización Internacional.
- Cuando dadas las circunstancias, el responsable o encargado del tratamiento recurra a las cláusulas tipo de protección de datos adoptadas por la Comisión o autoridad de control se debe permitir que puedan incluir dichas cláusulas tipo en un contrato más amplio. Asimismo, y siempre y cuando no contradigan de manera directa o indirecta las cláusulas tipo, podrán añadir otras cláusulas o garantías adicionales

Estas medidas deben asegurar un nivel de protección de datos adecuado. Es decir, cumplir con el contenido del REPD y la disponibilidad de acciones legales efectivas por parte de los interesados de sus derechos exigibles con los que obtener un resarcimiento pecuniario u obtener una reparación administrativa o judicial efectiva.

Las autorizaciones que se otorgaron de conformidad con la Directiva 95/46/CE por parte de una autoridad de control o por un Estado miembro continuarán siendo válidas hasta que dicha autoridad las tenga que modificar, sustituir o derogar

Binding Corporate Rules (BCR) o normas corporativas vinculantes

"Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta".

Siempre que se ofrezcan garantías de un nivel de protección adecuado para realizar transferencias internacionales de datos, se debe dar la posibilidad tanto a grupos empresariales como a la unión de empresas que se dediquen a un determinado sector, de utilizar **BCR o normas corporativas vinculantes autorizadas** para realizar dichas transferencias internaciones entre ellos.

La autoridad de control competente, siguiendo el mecanismo de coherencia del artículo 63 REPD basado en la cooperación de las autoridades de control con el fin de aplicar de forma coherente el RGPD, aprobará las BCR cuando:

- ❑ Sean aplicables, cumplidas y jurídicamente vinculantes por todos los miembros del grupo empresarial o grupo de empresas dedicadas a una actividad de un sector específico y de sus empleados.
- ❑ Otorguen a los interesados sus derechos exigibles en materia de protección de datos personales.

Contenido mínimo de las BCR

1. Forma de realizar el tratamiento.
2. Estructura del grupo o de la unión de empresas que realizan actividades de un sector específico.
3. Identificación y datos de contacto de cada uno de los miembros o integrantes de los mismos.
4. Transferencias internacionales de datos que se realizan, tipo de tratamiento, fines, interesados afectados y nombre del tercer/os países donde se produce la transferencia.
5. Garantía de su carácter jurídicamente vinculante (interno y externo).
6. Aplicación de los principios generales del RGPD, haciendo especial mención a la limitación de la finalidad y minimización de los datos.
7. Períodos de conservación de los datos personales, cumpliendo con el principio de calidad de los datos y la protección desde el diseño.
8. Garantía del tratamiento de categorías especiales de datos y las medidas para asegurarlos, en el caso de datos especialmente sensibles.
9. Niveles adecuados de protección exigidos por el RGPD, en aquellas transferencias que se realicen posteriormente a organismos no vinculados a las BCR.
10. Información sobre los derechos de los interesados, así como los medios para ejercerlos.
11. Información a los interesados sobre su derecho a presentar reclamación ante la autoridad de control competente, así como ante los tribunales competentes de los Estados miembros, tanto por violación de sus derechos, como para solicitar la reparación del mismo o indemnización debido a la vulneración de las BCR.
12. Aceptación por parte del responsable o encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por violación o vulneración de las BCR por un miembro no establecido en la Unión. El responsable o encargado el tratamiento será exonerado de responsabilidad si se demuestra que el origen de los daños provocados no se puede imputar a dicho miembro.
13. Funciones que tiene el delegado de protección de datos que se designe o cualquier persona o entidad que lleve a cabo la supervisión del cumplimiento de las BCR, la formación y el procedimiento y tramitación de las reclamaciones.
14. Establecimiento de mecanismos que garanticen el cumplimiento de las BCR (auditorías de protección de datos, acciones correctivas para proteger los derechos de los interesados, etc.).
15. Formación en materia de protección de datos al personal con acceso a datos personales.
16. Mecanismo para comunicar y registrar modificaciones introducidas en las normas y notificar esas modificaciones a la autoridad de control.
17. Cooperación con la autoridad de control para garantizar que se da cumplimiento de las BCR por los integrantes del mismo.
18. Procedimiento para informar a la autoridad de control de aquellos requisitos jurídicos que sean de aplicación en un tercer país a un miembro de las BCR y que pueda afectar las garantías establecidas en el mismo.
19. Por otro lado, la Comisión tendrá el poder para especificar cuál será el formato, así como los procedimientos que se deben establecer para el intercambio de información de las BCR entre los responsables, encargados y autoridades de control.

Comunicaciones o transferencias de datos no autorizadas por el derecho de la Unión y excepciones

En ocasiones podemos encontrarnos con situaciones algo más complejas donde se exija, mediante sentencia que proceda de un órgano jurisdiccional o mediante una decisión de una autoridad administrativa de un tercer país, que el responsable o encargado transfiera datos personales sin ser autorizado por el Derecho de la Unión. En estos casos, dicha transferencia o comunicación de datos será reconocida siempre que se base en un acuerdo internacional. Por ejemplo, los tratados de asistencia jurídica mutua entre un Estado miembro y un tercer país fuera de la Unión.

El REPD, en su artículo 49, establece una serie de excepciones

Que el interesado otorgue explícitamente su consentimiento para realizar dicha transferencia. Debe ser informado de los posibles riesgos que puede traer consigo debido a la ausencia de una decisión de adecuación por parte de la Comisión y la ausencia de garantías adecuadas recogidas en el artículo 46 RGPD.

Que la transferencia sea necesaria para la ejecución de un contrato entre el responsable y el interesado, así como para la ejecución de medidas precontractuales a solicitud del interesado

Que la transferencia sea necesaria para la ejecución o celebración de un contrato entre el responsable del tratamiento y una persona física o jurídica diferente, siempre que sea en interés del interesado

Que la transferencia sea necesaria por razones de interés público. El interés público será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento

Que la transferencia sea necesaria para la correcta formulación, ejercicio o defensa de reclamaciones

Que la transferencia sea necesaria para proteger intereses vitales del interesado o de otras personas, en aquellos casos en los que el mismo esté física o jurídicamente incapacitado para dar su consentimiento

Que la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta

Si no se está en las excepciones

Asimismo, encontramos otra posibilidad de realizar una transferencia internacional. Tiene lugar cuando no estemos en ninguna de las excepciones anteriormente comentadas y, además, nos encontremos ante la ausencia de una decisión de adecuación por parte de la Comisión, ausencia de garantías adecuadas o ausencia de BCR. En estos casos, **solo se podrá llevar a cabo**:

- ❑Si no es repetitiva y afecta a un número limitado de interesados.
- ❑Además, tiene que ser necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento de datos siempre que no prevalezcan derechos, libertades e intereses de los interesados.
- ❑Siempre que el responsable evalúe las circunstancias que tienen lugar en la transferencia, y en función de ellas ofrezca garantías adecuadas en materia de protección de datos.
- ❑El responsable debe informar a la autoridad de control de la transferencia.
- ❑Deber de información de los artículos 13 y 14 RGPD.
- ❑Se informará a los interesados de la transferencia y de cuáles son esos intereses legítimos imperiosos perseguidos por el responsable

Delegado Protección Datos "DPO"

No aparece definido en el REPD; sin embargo sí se ha regulado con todo detalle en los artículos 37 a 39 cuándo deberá designarse, la posición que debe ocupar y las funciones que se le atribuyen. Asimismo, el 13 de diciembre de 2016, el GT29 ha publicado varias directrices. Grupo de Trabajo del Artículo 29, 13/12/2016) en orden a aclarar la naturaleza de esta figura.

Obligatorio

- Autoridades u organismos públicos que realicen tratamientos de datos, con excepción de los juzgados y Tribunales en el ejercicio de su actividad jurisdiccional. En este sentido, el GT29 aclara que la noción de "autoridad u organismo público" debe determinarse con arreglo a la legislación nacional. De este modo, se incluyen las autoridades nacionales, regionales y locales, pero el concepto, según las leyes nacionales aplicables, puede incluir también una serie de **organismos que se rigen por derecho público (Colegio de Graduados Sociales)**. En consecuencia, el delegado también debería ser nombrado en entidades de derecho público o privado que operen en sectores tales como servicios de transporte público, suministro de agua y energía, infraestructuras ferroviarias, servicio público de radiodifusión, vivienda pública o los **órganos disciplinarios de las profesiones reguladas**, de conformidad con la legislación nacional.
- En este sentido, el GT29 justifica su interpretación sobre la base de que los interesados pueden encontrarse en una posición de inferioridad similar a la de cuando sus datos son tratados por una autoridad u organismo público. En particular, los datos pueden ser tratados con fines similares y los ciudadanos no suelen tener ningún margen de maniobra en el modo en que serán tratados sus datos y, por lo tanto, la designación del delegado puede constituir una garantía adicional de protección.
- Cuando el objeto principal del negocio del responsable o del encargado se encuentre más fundamentado en actividades de tratamiento que en virtud de su naturaleza, alcance y/o finalidad requieran operaciones habituales y sistemáticas de monitorización a gran escala de los titulares de los datos. Como ejemplo de actividades que quedarían integradas en esta categoría, podemos identificar tratamientos basados en tecnologías de Big Data, Internet de las cosas, elaboración de perfiles y segmentación de mercados, análisis de solvencia, seguros, etc.

De interés sobre DPO

- Cuando el objeto principal del negocio del responsable o del encargado se encuentre fundamentado en **actividades de tratamiento** impliquen el **manejo a gran escala de categorías especiales de datos** indicadas en el artículo 9.1 REPD y de datos relativos a condenas en infracciones penales.
- En el ámbito de un **grupo empresarial** se prevé la posibilidad de que se pueda nombrar a un **único delegado**, siempre y cuando sea accesible desde cada establecimiento.
- En relación al **ámbito público** también podrá designarse **un único delegado para varias autoridades u organismos**, atendiendo a la estructura organizativa y tamaño de cada entidad.
- Finalmente el GT29 identifica que **si un encargado cumple los criterios de designación obligatoria del delegado, su correspondiente responsable no está necesariamente obligado a nombrar esta figura pero sí identifica que puede ser una buena práctica**.
- *Como ejemplo, se hace referencia al caso de una pequeña empresa familiar dedicada a la distribución de electrodomésticos en una única ciudad que utiliza los servicios de un encargado cuya actividad principal es la de proporcionar servicios de análisis de sitios web y asistencia con publicidad y marketing comportamental. En este ámbito, las actividades de la empresa familiar y sus clientes no generan el tratamiento de datos a gran escala, teniendo en cuenta el reducido número de clientes y las actividades relativamente limitadas. Sin embargo, las actividades del encargado, teniendo muchos clientes como esta pequeña empresa y considerada su actividad en conjunto, sí se corresponde con un tratamiento a gran escala. Por consiguiente, el encargado debe designar un delegado, no estando obligada la propia empresa familiar*.

DPO Voluntariedad

- Posibilidad de **nombrar un delegado** por parte del responsable, encargado o las asociaciones u organismos que representen a categorías de responsables o encargados.
- Su nombramiento será voluntario, sin embargo se deja la puerta abierta a que el Derecho de la Unión o de los Estados miembros pueda exigir que deba nombrarse en otras situaciones. Asimismo, en las Directrices emitidas por el GT29 relativas al delegado de protección de datos se fomentan estos esfuerzos voluntarios

Requisitos del DPO

- El REPD prevé que el delegado podrá encontrarse **integrado en la plantilla** del responsable o del encargado o desempeñar sus servicios en el ámbito de una prestación de servicios. Asimismo, su identidad debe ser objeto de publicidad y de comunicación a la autoridad de control.
- El responsable, encargado u organización que deba designar un delegado debe analizar las cualidades profesionales de la persona que vaya a desempeñar el cargo y revisar que reúne los siguientes requisitos mínimos:
- Conocimientos especializados del Derecho en materia de protección de datos.
- Experiencia profesional en el ámbito práctico de protección de datos.
- Capacidad para desempeñar las funciones que le atribuye el RGPD.
- En el ámbito de delegados externos designados sobre la base de un contrato de prestación de servicios, el GT29 señala que es esencial que cada miembro de la organización que ejerza las funciones de delegado cumpla todos los requisitos (por ejemplo, es esencial que nadie tenga un conflicto de intereses). Es igualmente importante que cada uno de esos miembros esté protegido por las disposiciones del REPD (por ejemplo, que no pueda resolverse el contrato por el ejercicio correcto de funciones del delegado, ni tampoco despido injustificado de ningún miembro individual de la organización que lleva a cabo tareas en calidad de delegado). Al mismo tiempo, las habilidades individuales y las fortalezas se pueden combinar para que varias personas, trabajando en equipo, puedan servir más eficientemente a sus clientes.
- **En aras de la seguridad jurídica y una buena organización, se recomienda tener una asignación clara de tareas dentro del equipo de delegados y asignar a única persona como contacto principal y persona a cargo de cada cliente. Estos aspectos, en cualquier caso, deberían especificarse de manera clara en el contrato de prestación de servicios**.

Posición ante la protección de datos del DPO

Garantías (art.38 REPG)

- Garantías de que participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales. El GT29 identifica, en este ámbito, que la organización debe garantizar, por ejemplo, que se invite al delegado a participar regularmente en reuniones de dirección; se requiera su presencia cuando se adopten decisiones con implicaciones de protección de datos y se le facilite toda la información pertinente para que pueda proporcionar el asesoramiento adecuado; se tenga siempre en cuenta su opinión y, en caso de desacuerdo que, como buena práctica, se deje constancia de las razones para no seguir su criterio.
- Apoyo el desempeño de las funciones atribuidas por el RGPD, debiendo facilitarle los recursos necesarios para el desempeño de las mismas, el acceso a los datos personales y a las operaciones de tratamiento y el mantenimiento de sus conocimientos especializados. En este aspecto, las directrices definidas por el GT29, apuntan a que el delegado debe disponer de tiempo suficiente para que pueda cumplir sus funciones. Esto es particularmente importante cuando el delegado se nombre a tiempo parcial o cuando realice otras tareas; de lo contrario, las tareas conflictivas podrían dar lugar a que se descuiden sus deberes como delegado. Asimismo, se considera como buenas prácticas que se establezca un porcentaje de tiempo para la función de delegado cuando se realiza a tiempo parcial, se determine el tiempo necesario para llevar a cabo su función, el nivel apropiado de prioridad para sus tareas y la elaboración de un plan de trabajo.
- Asimismo, el GT29 identifica que se le debe dar el apoyo adecuado en términos de recursos financieros, infraestructura (locales, instalaciones, equipo) y personal, cuando corresponda. También debe ofrecerse al delegado la oportunidad de mantenerse al día en lo que respecta a la evolución de la protección de datos mediante formación adecuada.
- Garantía de independencia en su actuación de modo que se avale que el delegado no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones. Asimismo, el RGPD prevé que no podrá ser destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, respondiendo de su actividad únicamente y de manera directa al más alto nivel jerárquico del responsable o encargado.
- El GT29 señala que la autonomía del delegado no significa que tenga poderes de decisión que vayan más allá de sus funciones, puesto que el responsable o encargado sigue siendo responsable del cumplimiento de la normativa y debe ser capaz de demostrarlo, de modo que si se deben adoptar decisiones que se consideran incompatibles con el RGPD y el consejo del delegado, este último debe poder emitir su opinión discrepante de manera clara dirigida a los responsables de la toma de decisiones.
- Contacto directo de los interesados con el delegado de protección de datos en relación a las cuestiones relativas al tratamiento de sus datos y al ejercicio de sus derechos. El objetivo de este requisito es garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades de control puedan contactar fácil y directamente con el delegado sin tener que ponerse en contacto con otra parte de la organización. Los datos de contacto del delegado, según interpreta el GT29, deben incluir información que permita contactar de una manera fácil (dirección postal, número de teléfono y correo electrónico dedicados). Asimismo, si resulta más apropiado, también se puede habilitar una línea directa o un formulario de contacto dedicados dirigidos al delegado en la página web de una organización. Por último, el RGPD no exige que los datos de contacto publicados incluyan el nombre del delegado, si bien puede el GT29 señala que puede constituir una buena práctica dejando en manos de responsables y encargados si puede ser necesario o resultar de utilidad.
- Mantenimiento del deber de secreto o la confidencialidad por parte del delegado en relación al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros. Sin embargo, la obligación de secreto o la confidencialidad no prohíbe que el delegado contacte y solicite asesoramiento a la autoridad supervisora de manera directa.
- El delegado de protección de datos puede tener asignadas otras funciones dentro de la entidad, sin embargo el responsable o encargado debe garantizar que dichas funciones no den lugar a conflicto de intereses.

Funciones del DPO

- Función informativa y de asesoramiento al responsable o al encargado y los empleados de la organización, en relación a las obligaciones en materia de protección de datos, de conformidad con el RGPD o con otra normativa de la Unión de los Estados miembros
- Función de supervisión del cumplimiento normativo en el ámbito de la normativa y las políticas implantadas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes.
- Función de asesoramiento que se le solicite en relación a la evaluación de impacto y supervisión de su aplicación.
- Función de cooperación con la autoridad de control.
- Actuar como punto de contacto o enlace de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa y realizar consultas, en su caso, sobre cualquier otro asunto

Responsabilidad del DPO

En relación a la responsabilidad del delegado, el GT29 identifica que el ejercicio de la función de supervisión del cumplimiento no implica que asuma responsabilidad personal cuando exista un caso de incumplimiento.

El REPD deja claro que es el responsable o encargado y no el delegado quien debe aplicar las medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el tratamiento se realiza de conformidad con el REPD. El cumplimiento de protección de datos es una responsabilidad corporativa del responsable o del encargado y no del delegado

Recursos

Los artículos 77 a 82 RGPD identifican los **recursos de que disponen los interesados** para poder defender sus derechos o denunciar las infracciones de las previsiones del RGPD, siendo los siguientes:

1. Derecho a presentar una reclamación ante una autoridad de control
2. Derecho a la tutela judicial efectiva contra una autoridad de control
3. Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento
4. Representación de los interesados
5. Suspensión de los procedimientos
6. Derecho a indemnización
7. Responsabilidad en relación a la indemnización

Condiciones generales para la imposición de multas administrativas

- A fin de reforzar la aplicación de las normas del RGPD, cualquier infracción viene castigada con sanciones, incluidas multas administrativas. Asimismo, pueden también establecerse medidas adecuadas impuestas por la autoridad de control en el ejercicio de sus poderes correctivos. Al igual que sucede en nuestro sistema actual (hasta que sea de aplicación el RGPD), el considerando (148), hace referencia al apercibimiento, para identificar que en caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. En el artículo 83 RGPD se identifican las características principales que se predican respecto de una multa administrativa de tipo económico debiendo ser, en cada caso, **efectivas, proporcionadas y disuasorias**.
- En relación a las infracciones de las autoridades y organismos públicos, el RGPD contiene la previsión de que cada Estado miembro podrá establecer normas, en la medida que su ordenamiento lo permita, con la finalidad de imponerles multas administrativas, sin perjuicio de los poderes correctivos de las autoridades de control. En España, estimamos que no podrán establecerse este tipo de normas y se continuará con un sistema similar al actual de Procedimiento de declaración de Infracción de Administraciones Públicas.
- En cualquier caso, el RGPD prevé que el ejercicio de los poderes de la autoridad de control estará sujeto a garantías procesales adecuadas, de conformidad con el Derecho de la Unión y de los Estados miembros.

Criterios de graduación

Los criterios que deben ser tenidos en cuenta para la graduación de una multa, en atención a las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el ejercicio de los poderes correctivos de las autoridades de control son los siguientes:

- ❑ Naturaleza, gravedad y duración de la infracción, alcance o fines del tratamiento, número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido.
- ❑ La intencionalidad o negligencia en la infracción.
- ❑ Las medidas tomadas para paliar los daños y perjuicios sufridos.
- ❑ El grado de responsabilidad del sujeto infractor, teniendo en cuenta las medidas técnicas u organizativas apropiadas que hubiese aplicado.
- ❑ Reincidencia o infracciones previamente cometidas.
- ❑ Grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.
- ❑ Las categorías de los datos de carácter personal afectados por la infracción.
- ❑ La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el infractor notificó la infracción y, en tal caso, en qué medida.
- ❑ Cumplimiento de medidas correctivas ordenadas previamente en relación con la naturaleza de la infracción.
- ❑ Adhesión a códigos de conducta o a mecanismos de certificación.
- ❑ Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Multas administrativas de carácter económico (10m)

Infracción de las obligaciones del responsable y del encargado

- ❑ Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.
- ❑ Tratamiento que no requiere identificación.
- ❑ Protección de datos desde el diseño y por defecto.
- ❑ Corresponsables del tratamiento.
- ❑ Representantes de responsables o encargados del tratamiento no establecidos en la Unión.
- ❑ Encargado del tratamiento.
- ❑ Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.
- ❑ Registro de las actividades de tratamiento.
- ❑ Cooperación con la autoridad de control.
- ❑ Seguridad del tratamiento.
- ❑ Notificación de una violación de la seguridad de los datos personales a la autoridad de control.
- ❑ Comunicación de una violación de la seguridad de los datos personales al interesado.
- ❑ Evaluación de impacto relativa a la protección de datos.
- ❑ Consulta previa.
- ❑ Designación del delegado de protección de datos.
- ❑ Posición del delegado de protección de datos.
- ❑ Funciones del delegado de protección de datos.
- ❑ Certificación.
- ❑ Organismo de certificación.

Multa administrativa de 10.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

Multas administrativas de carácter económico (10m)

Infracción de las obligaciones de los organismos de certificación

Relacionadas con la expedición de la certificación y su acreditación y funcionamiento

Infracción de las obligaciones de los organismos de supervisión de los códigos de conducta

- En la versión del RGPD publicada en castellano, el artículo 83.4 c) tiene la siguiente redacción: *"c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4".* Sin embargo, en la versión publicada en inglés la redacción es la siguiente: *"(c) the obligations of the monitoring body pursuant to Article 41(4)".* Puede apreciarse, por tanto, que existe un error de traducción, puesto que si tomamos en consideración el literal de la versión en castellano, no resulta lógico que la autoridad de control pueda sancionarse a sí misma (en España, la AEPD). En cualquier caso, en el presente estudio se toma como versión válida la versión en inglés traduciéndose como "organismo supervisor", de modo que posteriormente se estará a la Corrección de errores del Reglamento para sustituirlo por la traducción oficial.
- Relacionadas con la adopción de medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este e información de dichas medidas y de las razones de las mismas a la autoridad de control competente.

Multa administrativa de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía (I)

Solucyl Consultores Tecnológicos, S.L.L.

JUSTICIA SOCIAL

Wolters Kluwer | A3 Software

Infracción de los principios básicos para el tratamiento

Incluidas las condiciones para el consentimiento, la licitud del tratamiento y el tratamiento de categorías especiales de datos personales.

Los derechos de los interesados

- **Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.**
- **Información que deberá facilitarse cuando los datos personales se obtengan del interesado.**
- **Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.**
- **Derecho de acceso del interesado.**
- **Derecho de rectificación.**
- **Derecho de supresión (“el derecho al olvido”).**
- **Derecho a la limitación del tratamiento.**
- **Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.**
- **Derecho a la portabilidad de los datos.**
- **Derecho de oposición.**
- **Decisiones individuales automatizadas, incluida la elaboración de perfiles.**

(II)

Las transferencias internacionales de datos

A un destinatario en un tercer país o una organización internacional.

Obligaciones relativas a disposiciones relativas a situaciones específicas de tratamiento

Que se adopten por los Estados.

El incumplimiento de una resolución

O de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos impuesta por una autoridad de control impuesta como medida correctiva o el no facilitar acceso en virtud de los poderes de investigación de la citada autoridad

Multa administrativa de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

Solucyl Consultores Tecnológicos, S.L.L.

Wolters Kluwer | A3 Software

Incumplimiento de las medidas correctivas impuestas por una autoridad de control

Se reproducen los poderes correctivos de la autoridad de control, analizados en el tema dedicado a la autoridad, siguiendo la numeración del RGPD para una mayor claridad en el seguimiento de la tipificación de las infracciones.

- ❑ Sancionar con una advertencia cuando prevea que un responsable o encargado pueden infringir el RGPD.
- ❑ Sancionar con apercibimiento cuando el tratamiento de un responsable o encargado hayan infringido el RGPD.
- ❑ Ordenar al responsable o encargado que atiendan las solicitudes de ejercicio de los derechos del interesado.
- ❑ Ordenar al responsable o encargado del tratamiento que el tratamiento se ajuste al RGPD, pudiendo concederle, si procede, que lo lleve a cabo de una determinada manera y en el plazo especificado.
- ❑ Ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales.
- ❑ Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- ❑ Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales.
- ❑ Retirar una certificación u ordenar al organismo de certificación que la retire mandar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos requeridos para la misma.
- ❑ Imponer una multa administrativa, adicionalmente o en sustitución de las medidas correctivas anteriores, atendiendo a las circunstancias de cada caso.

Sanciones

- Las normas previstas en el RGPD relativas a sanciones aplicables a las infracciones, no constituirán, de momento, un listado cerrado puesto que el artículo 84 RLOPD.
- Esto faculta a los Estados miembros a desarrollar normas que, de manera particular, contemplen sanciones que no lleven aparejada una multa administrativa que, en cualquier caso deberán ser efectivas, proporcionadas y disuasorias.
- Las nuevas normas que adopte un estado serán comunicadas a la Comisión a más tardar el 25 de mayo de 2018

Resumen Cumplimiento RGPD

1) Designación del **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, identificar a la/s persona/s responsables de COORDINAR LA ADAPTACIÓN.
2) Elaborar el **REGISTRO ACTIVIDADES DE TRATAMIENTO** *(servicio de solicitud de copia de la inscripción como ayuda),* teniendo en cuenta su finalidad y la base jurídica.
3) Realizar un **ANÁLISIS DE RIESGOS**. Revisar MEDIDAS DE SEGURIDAD a la luz de los resultados del análisis de riesgos.
4) Establecer mecanismos y procedimiento de **NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD**.
5) A partir de los resultados del análisis de riesgos, realizar, en su caso, una **EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS**

1) Adecuar los **FORMULARIOS** *derecho de información*
2) Adaptar los **MECANISMOS Y PROCEDIMIENTOS** para el ejercicio de derechos
3) Valorar si los **ENCARGADOS** ofrecen garantías y *adaptación de contratos*
4) Elaborar / Adaptar **POLÍTICA DE PRIVACIDAD**

En Paralelo

Muchas Gracias ...

Solucyl
Consultores Tecnológicos, S.L.L.

Wolters Kluwer | A3 Software