**Cumplimiento de las obligaciones**

**En esta sección te explicamos las obligaciones que deben cumplir aquellos que tratan datos personales (organizaciones, empresas, administraciones públicas) y te ofrecemos diversos materiales de ayuda para cumplir con ella.**

Recuerda que si tratas datos o información sobre personas físicas que permitan su identificación, los utilizas con fines determinados y tomas decisiones relacionadas con los fines para los que utilizas estos datos personales o los medios en los que llevas a cabo el almacenamiento y la forma de procesar los datos, **eres “el responsable” de la actividad de tratamiento**estos datos.

Si almacenas o procesas datos o información sobre personas físicas siguiendo las instrucciones de quien toma decisiones sobre los fines y los medios en los que los datos son procesados (“el responsable”) **eres “el encargado” de la actividad de tratamiento** de estos datos.

Por el contrario, si almacenas o procesas datos personales únicamente en el ejercicio de tus actividades personales o domésticas, los requisitos de la normativa de protección de datos no son de aplicación para en el ámbito de dichas actividades.

Para cada actividad de tratamiento de datos personales que llevas a cabo como responsable o en la que participas como encargado, debes tener en cuenta las obligaciones que el RGPD y la LOPDGDD te exigen para proteger a las personas físicas cuyos datos estás tratando.

Para comenzar, te recomendamos la consulta de este documento básico para cumplir con los requisitos que exige la normativa de protección de datos:

* [**Hoja de ruta básica para la aplicación del RGPD y la LOPDGDD**](https://www.aepd.es/es/documento/hoja-de-ruta.pdf)

También tienes a tu disposición nuestros asistentes para el cumplimiento normativo[**FACILITA\_RGPD**](https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd) y [**FACILITA\_EMPRENDE**](https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-emprende).

Ten cuidado con las ofertas a coste cero y otro tipo de prácticas fraudulentas asociadas, como difundir que se está obligado a contratar un DPD en todos los casos o la oferta de servicios innecesarios, entre otras.

[**ADECUACIÓN A LA NORMATIVA 'COSTE CERO' Y OTRAS PRÁCTICAS FRAUDULENTAS**](https://www.aepd.es/es/documento/coste-cero.pdf)



**Principios**

El Reglamento General de Protección de Datos señala un conjunto de principios que los responsables y encargados del tratamiento deben observar al tratar datos personales:

* **Principio de “licitud, transparencia y lealtad”, que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.**
* **Principio de “finalidad” que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.**
* **Principio de “minimización de datos”, es decir, aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.**
* **Principio de “exactitud”, que obliga a los responsables a disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.**
* **Principio de “limitación del plazo de conservación” que constituye una de las materializaciones del principio de minimización. La conservación de esos datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados.**
* **Principio de “seguridad” que impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.**
* **Principio de “responsabilidad activa” o “responsabilidad demostrada” que obliga a los responsables a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que el responsable pueda, tanto garantizar como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.**

**Medidas de cumplimiento**

Para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados, a la vez que para demostrar el cumplimiento, el RGPD incorpora una serie de obligaciones en cumplimiento del principio de responsabilidad proactiva. A continuación, se detallan las obligaciones del responsable, sin perjuicio de otras que pudieran ser necesarias para el objetivo de garantizar y proteger los derechos y libertades de las personas físicas cuyos datos son tratados.

* [**Registro de actividades de tratamiento**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/actividades-tratamiento)
* [**Inventario de actividades de tratamiento**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/inventario-de-actividades-de-tratamiento)
* [**Designación de un delegado de protección de datos**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/designacion-delegado-proteccion-datos)
* [**Evaluación del riesgo que, para los derechos y libertades de los interesados, podría suponer un tratamiento de datos personales**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/evaluacion-del-riesgo-que-un)
* [**Realización de evaluaciones de impacto para la protección de datos**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/evaluaciones-de-impacto)
* [**Consulta previa**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/consulta-previa)
* [**Protección de datos desde el diseño**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-desde-el-diseno)
* [**Protección de datos por defecto**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-por-defecto)
* [**Seguridad de los tratamientos de datos**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/seguridad-de-los-tratamientos)
* [**Notificación de brechas de datos personales a la Autoridad de Control**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion)
* [**Comunicación de brechas de datos personales a los interesados**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/comunicacion-de-brechas-de-datos)
* [**Códigos de conducta**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta)
* [**Establecimiento de garantías para las transferencias de datos personales a terceros países u organizaciones internacionales**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales)

**Registro de actividades de tratamiento**

Una de las herramientas que el RGPD exige a los responsables para demostrar la conformidad con el RGPD es el mantenimiento de los registros de actividades de tratamientos de datos que tienen bajo su responsabilidad y control, teniendo en cuenta la obligada colaboración con la Autoridad de Control que exige poner a su disposición dichos registros de operaciones de tratamiento para facilitar las actividades de supervisión realizadas en el ámbito de los poderes que el RGPD le otorga.

El RGPD y la LOPDGDD exigen un contenido mínimo que deberá ser tenido en cuenta por el responsable:

* **el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;**
* **los fines del tratamiento;**
* **una descripción de las categorías de interesados y de las categorías de datos personales;**
* **las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;**
* **en su caso, las 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 indicadas en el artículo 49, apartado 1, párrafo segundo2, 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**

El contenido del Registro de Actividades de Tratamiento constituye una información mínima exigible. Este registro podría integrarse y formar parte de los catálogos de procesos que ya existiesen en la entidad, incluyendo toda la información que el responsable considere necesaria para proteger los derechos y libertades de las personas físicas y poder demostrar cumplimiento atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los posibles orígenes de los riesgos que dicho tratamiento pudiera suponer para los interesados. El registro podría incluir aspectos que faciliten la aplicación efectiva de la responsabilidad proactiva como: análisis de riesgos para los derechos y libertades realizados, la descripción sistemática del tratamiento, los sistemas de información sobre los que se apoya, la descripción de la identidad de los encargados del tratamiento, las garantías previstas para llevar a cabo transferencias internacionales de datos, información de contacto de las personas o los departamentos de la organización que se encuentran implicados en las operaciones de tratamiento, etc.

En el caso de dar acceso al contenido del Registro de Actividades de Tratamiento, y con relación a una posible descripción general de las medidas técnicas y organizativas de seguridad, debe evitarse desvelar cualquier información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad. En este caso, se recomienda contar con el Responsable de Seguridad o CISO con carácter previo a la publicación de dicha descripción general o, en su caso, utilizar una referencia general a los estándares de seguridad utilizados.

Para ayudarte en la elaboración del registro de actividades de tratamiento puedes utilizar la herramienta [**FACILITA\_RGPD**](https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd).

**Inventario de actividades de tratamiento**

Además del registro de actividades de tratamiento, las entidades señaladas en la LOPDGDD en su artículo 77.1, con fines de transparencia (Art. 6.bis Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno), deberán hacer público el inventario de sus actividades de tratamiento de manera que sea accesible por medios electrónicos (Art. 31.2 LOPDGDD) donde se incluya, para cada actividad de tratamiento:

* **el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;**
* **la base jurídica del tratamiento;**
* **los fines del tratamiento;**
* **una descripción de las categorías de interesados y de las categorías de datos personales;**
* **las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;**
* **en su caso, las 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 indicadas en el artículo 49, apartado 1, párrafo segundo2, 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. En dicha descripción general debe evitarse cualquier información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad. Se recomienda contar con el Responsable de Seguridad o CISO con carácter previo a la publicación de dicha descripción general o, en su caso, utilizar una referencia general a los estándares de seguridad utilizados.**

**Designación de un delegado de protección de datos**

El Reglamento general de protección de datos (RGPD) configura al Delegado de Protección de Datos (DPD) como una figura clave en el modelo de su cumplimiento para lo que debe ser conocedor del Derecho y la práctica en materia de protección de datos. El RGPD establece en su artículo 37 cuando un responsable o encargado debe proceder a su designación:

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

Así mismo, el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos personales y garantía de los derechos digitales (LOPDPGDD) detalla los responsables y encargados que, en todo caso, **han de proceder a la designación obligatoria de DPD**:

* **Los colegios profesionales y sus consejos generales.**
* **Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.**
* **Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.**
* **Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de las personas usuarias del servicio.**
* **Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.**
* **Los establecimientos financieros de crédito.**
* **Las entidades aseguradoras y reaseguradoras.**
* **Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.**
* **Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.**
* **Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.**
* **Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de las personas afectadas o realicen actividades que impliquen la elaboración de perfiles de las mismas.**
* **Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.**
* **Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.**
* **Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.**
* **Las personas operadoras que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.**
* **Las empresas de seguridad privada.**
* **Las federaciones deportivas cuando traten datos de menores de edad.**

Las entidades responsables o encargadas del tratamiento no incluidas en el párrafo anterior podrán designar de manera voluntaria un DPD que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la citada ley orgánica.

La entidad responsable o encargada del tratamiento que designe un DPD tiene la obligación, de acuerdo con el artículo 37.7 del RGPD:

* **Comunicarlo a la autoridad de control en el plazo 10 días.**
* **Publicitar su existencia a través de medios electrónicos.**

La Agencia Española de Protección de Datos **pone a disposición** de los responsables y encargados de tratamiento que designen DPD, a través de su [**Sede Electrónica**](https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf) el:

[**Formulario de Comunicación de persona delegada de protección de datos**](https://sedeagpd.gob.es/sede-electronica-web/vistas/formDelegadoProteccionDatos/procedimientoDelegadoProteccion.jsf)

La lista de los DPD comunicados a la Agencia española de Protección de Datos se encuentra **publicada**en su Sede Electrónica y es accesible desde este enlace:

[**Consulta de los datos de contacto de los Delegados de Protección de Datos**](https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf)

Los artículos 38 y 39 del RGPD, así como los artículos 36 y 37 de la LOPDPGDD detallan la **posición**y **funciones**de los DPD, entre ellas las de informar y asesorar al responsable o al encargado de las obligaciones que establece el RGPD y supervisar su cumplimiento, que ejercerán de manera independiente, además de actuar como punto de contacto con la Agencia Española de Protección de Datos.

Información más detallada en las que sobre su designación, cualificación, posición y funciones de los DPD en las [**Directrices de los delegados de protección de datos**](https://www.aepd.es/es/documento/wp243rev01-es.pdf) del Comité Europeo de Protección de Datos ha publicado este documento.

**Certificación de DPD**

Con la finalidad de ofrecer seguridad y fiabilidad tanto a las personas profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones o que necesitan contratar los servicios de una persona profesional cualificada, la AEPD ha optado por promover un [**Esquema de Certificación de DPD**](https://www.aepd.es/es/documento/esquema-aepd-dpd.pdf).

# Evaluación del riesgo que un tratamiento de datos personales puede suponer para los derechos y libertades de las personas

**El RGPD obliga al responsable llevar a cabo la evaluación de los riesgos que, para los derechos y libertades de las personas físicas, un tratamiento pudiera implicar. Para ello es necesario, en primer lugar, identificar el riesgo y su origen, llevar a cabo su evaluación y la consecuente gestión de las medidas que pudieran ser necesarias a fin de evitar las posibles consecuencias negativas que el tratamiento pudiera implicar para los interesados.**

En esta línea, la normativa de protección de datos proporciona una lista de posibles riesgos que no debe ser interpretada de manera excluyente. Es decir, no se trata de una lista cerrada, sino que el responsable debe llevar a cabo dicha evaluación del riesgo de acuerdo con la naturaleza, el contexto, el alcance y los fines de cada tratamiento de datos de los que es responsable e incluir todos aquellos que identifique. Ejemplos de la normativa sobre las consecuencias que un tratamiento de datos puede tener sobre las personas son: agresión a sus derechos y libertades fundamentales, irreversibilidad de sus efectos, compromiso de las categorías especiales de datos, daños sociales, morales o materiales, incluyendo perjuicios financieros, pérdida de control de los propios datos, robo de identidad, con especial atención a las personas en situación de especial vulnerabilidad.

Para evaluar los riesgos que un tratamiento de datos personales representa para los derechos y libertades de los interesados cuyos datos son tratados es preciso llevar a cabo, en primer lugar, la identificación de dichos riesgos para, posteriormente, gestionarlos a lo largo de todo el ciclo de vida del tratamiento, es decir, desde su diseño hasta que la actividad de tratamiento deje de ser necesaria.

[**Aquí**](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia) puede consultar recursos de ayuda para llevar a cabo la evaluación del riesgo para los derechos y libertades de las personas físicas.

**Realización de evaluaciones de impacto de protección de datos**

El RGPD introduce el concepto de Evaluación de Impacto relativa a la Protección de Datos (EIPD) y obliga a las Autoridades de Control a establecer listas orientativas de tratamientos que no requieren EIPD, así como de tratamientos que sí requieren su realización.  
Puede consultar las listas orientativas de tratamientos que no requieren EIPD publicadas por la AEPD y aprobadas por el EDPB aquí:

[**Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)**](https://www.aepd.es/es/documento/listasdpia-35.5l.pdf)

Puede consultar la lista orientativa de tratamientos que requieren EIPD publicada por la AEPD y aprobada por el EDPB aquí:

[**Listas de tipos de tratamientos de datos que requieren Evaluación de impacto relativa a protección de datos (art 35.4)**](https://www.aepd.es/es/documento/listas-dpia-es-35-4.pdf)

Con carácter general, existe la obligación de llevar a cabo la realización de una EIPD siempre que el tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas. No obstante, con independencia de esta obligación, el responsable podrá llevar a cabo la EIPD cuando lo considere o valore necesario, **estas listas son orientativas y no restrictivas**.

Puede consultar los recursos de ayuda publicados por la AEPD para realizar la evaluación del riesgo y la EIPD en el [**área de actuación de innovación y tecnología de nuestra web**](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia).

* [**Gestión del riesgo y evaluación de impacto en tratamientos de datos personales**](https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf)
* [**Relación de tablas de la guía de Gestión del riesgo y evaluación de impacto en formato editable**](https://www.aepd.es/es/documento/relacion-tablas-guia-riesgo-eipd-tablas.odt)
* [**Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa**](https://www.aepd.es/es/documento/lista-verificacion-eipd-consulta-previa.docx)
* [**Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4)**](https://www.aepd.es/es/documento/listas-dpia-es-35-4.pdf)
* [**Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)**](https://www.aepd.es/es/documento/listasdpia-35.5l.pdf)
* [**Instrucción 1/2021 de la AEPD de directrices respecto de la función consultiva de la Agencia. Capitulo IV: Consultas Previas**](https://www.boe.es/boe/dias/2021/11/05/pdfs/BOE-A-2021-18134.pdf)
* [**Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas**](https://www.aepd.es/es/documento/modelo-informe-EIPD-AAPP.rtf)
* [**Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado**](https://www.aepd.es/es/documento/modelo-informe-eipd-sector-privado.rtf)
* [**EDPS: Guía para evaluar la proporcionalidad de los tratamientos en políticas y medidas legislativas**](https://www.aepd.es/es/documento/guia-evaluar-proporcionalidad-tratamientos-en-politicas-y-medidas-legislativas.pdf)
* [**EDPS: Guía para evaluar la necesidad de los tratamientos en políticas y medidas legislativas**](https://www.aepd.es/es/documento/guia-evaluar-necesidad-tratamientos-en-politicas-y-medidas-legislativas.pdf)
* [**Herramienta EVALUA-RIESGO para el análisis de los factores de riesgo**](https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd)
* [**Herramienta de ayuda para empresas que realicen un tratamiento de datos personales de escaso riesgo para el cumplimiento del RGPD: FACILITA-RGPD**](https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd)
* [**Herramienta para ayudar a las personas emprendedoras y startups tecnológicas a cumplir con la normativa de protección de datos: FACILITA-EMPRENDE**](https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-emprende)
* [**Herramienta básica para la realización de análisis de riesgos y evaluaciones de impacto en protección de datos**](https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd)

# Protección de datos desde el diseño

El RGPD exige a los responsables establecer las medidas técnicas y organizativas necesarias a lo largo de todo el ciclo de vida del tratamiento, tanto desde el momento inicial en que se lleva a cabo la definición del tratamiento y se determinan los medios como durante su puesta en marcha y funcionamiento habitual. Estas medidas y garantías deben establecerse atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como a los riesgos para los derechos y libertades de los interesados que pueda llegar a representar.

La protección de datos desde el diseño tiene por objetivo aplicar los principios de protección de datos en los procesos de diseño de los sistemas y procedimientos de la organización sobre los que se apoya el  tratamiento de los datos, con un fin eminentemente preventivo y orientado tanto a evitar posibles daños a las personas físicas como, de manera colateral, los perjuicios que para la organización podría suponer la modificación o el rediseño de los sistemas en los que se llevan a cabo los tratamientos, una vez desarrollados e implantados, como consecuencia de la identificación de errores de diseño que pudieran suponer daños o perjuicios a los interesados y a sus derechos y libertades.

Para más información sobre esta obligación, la AEPD ha publicado la guía de protección de datos desde el diseño que se encuentra disponible en el apartado web de [**innovación y tecnología**](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia) y que puede consultar en el siguiente enlace:

[**Guía de Privacidad desde el Diseño**](https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf)

Téngase en cuenta que las guías y herramientas de esta Agencia son recursos de ayuda al cumplimiento y que, en ningún caso, sustituyen a la obligación del responsable de aplicar cuantas medidas pudieran ser necesarias para garantizar, de manera efectiva, los derechos y libertades de las personas físicas cuyos datos se tratan, teniendo en cuenta la naturaleza, el alcance, el contexto, los fines del tratamiento así como los riesgos de diversa probabilidad, gravedad y origen que pudieran derivar de los tratamientos que se llevan a cabo.

# Protección de datos por defecto

El principio de protección de datos por defecto supone la puesta en práctica del principio de minimización de datos mediante las medidas técnicas y organizativas que garanticen, por defecto, que únicamente sean objeto de tratamiento los datos necesarios para los fines del mismo y que hubieran sido definidos en la etapa de diseño inicial.

El RGPD exige del responsable una configuración por defecto de los tratamientos que sea respetuosa con los principios de protección de datos, abogando por un procesamiento mínimamente intrusivo: mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación y mínima accesibilidad a datos personales. Todo ello, además, sin que sea necesaria la intervención del interesado para garantizar que estos mínimos se hayan establecido. De ahí que la Protección de datos por defecto no se limita a requisitos sobre programas o dispositivos, sino que afecta también al propio diseño del tratamiento, con independencia del soporte en el que este se desarrolle.

También deben ser tenidas en cuenta las opciones de configuración que pudieran definir la implementación concreta del tratamiento atendiendo a las decisiones que el propio interesado pudiera tomar acerca de cómo desea que sean tratados sus datos.

Para más información sobre esta obligación, la AEPD ha publicado la guía de protección de datos por defecto que se encuentra disponible en el [**apartado web de innovación y tecnología**](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia) y que puede consultar en el siguiente enlace:

[**Guía de Protección de Datos por Defecto**](https://www.aepd.es/es/documento/guia-proteccion-datos-por-defecto.pdf)

Junto con esta guía se pone a disposición de los responsables un conjunto de propuestas que pueden servirle de orientación a la hora de determinar algunas de las medidas de protección de datos por defecto aplicables a los tratamientos de datos personales que realicen en el marco de sus actividades:

[**Protección de datos por defecto: Listado de medidas**](https://www.aepd.es/es/documento/PDpD-listado-medidas.xlsx)

Téngase en cuenta que las guías y herramientas de esta Agencia son recursos de ayuda al cumplimiento y que, en ningún caso, sustituyen a la obligación del responsable de aplicar cuantas medidas pudieran ser necesarias para garantizar, de manera efectiva, los derechos y libertades de las personas físicas cuyos datos tratan, teniendo en cuenta la naturaleza, el alcance, el contexto, los fines del tratamiento así como los riesgos de diversa probabilidad, gravedad y origen que pudieran derivar de los tratamientos que se llevan a cabo.

**Seguridad de los tratamientos**

El artículo 32 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

A fin de mantener la seguridad de los tratamientos se exige al responsable evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. En dicha evaluación del riesgo deben tenerse en cuenta los riesgos que atenten contra los derechos y libertades de los interesados, especialmente sus derechos y libertades fundamentales.

Con el objetivo de seleccionar las medidas para gestionar el riesgo para los derechos y libertades, pueden utilizarse estándares de seguridad ya existentes en el mercado como la norma ISO 27000. Por su parte, las Administraciones Públicas deberán utilizar el Esquema Nacional de Seguridad para seleccionar las medidas que deban implantarse para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos. Con carácter general el estándar utilizado implicará:

* **La realización de un inventario de activos partiendo de la descripción sistemática del tratamiento**
* **La identificación de los riesgos, para los derechos y libertades de los interesados, asociados a los activos que consten en el inventario de activos**
* **La evaluación del riesgo para los derechos y libertades de los interesados**
* **La gestión de riesgos para los derechos y libertades de los interesados a lo largo del ciclo de vida del tratamiento**

Con el objetivo de ayudar en el análisis de riesgos orientado a determinar las medidas de seguridad, la AEPD ofrece indicaciones en la guía: [**Gestión de riesgo y evaluación de impacto en tratamientos de datos personales**](https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf), en particular en los capítulo VI y VIII.D.

**Notificación de brechas de datos personales a la Autoridad de Control**

**Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.**

**Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.**

**El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.**

**Con el objetivo de ayudar en la toma de decisiones, la AEPD ofrece la herramienta**[**ASESORA BRECHA**](https://www.aepd.es/es/guias-y-herramientas/herramientas/asesora-brecha)**.**

**El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo, y además cuando el riesgo sea alto el responsable también deberá**[**comunicar la brecha a las personas afectadas**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/comunicacion-de-brechas-de-datos)**conforme al artículo 34 del RGPD.**

**El plazo para notificar a la autoridad de control es de 72 horas desde que la organización tiene constancia de la brecha.**

**En el ámbito privado, los responsables del tratamiento afectados por una brecha de datos personales deberán notificar a la AEPD:**

* **Cuando su único establecimiento esté localizado en España.**
* **Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.**
* **Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.**
* **Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.**

**En el ámbito público, con carácter general las AAPP deben notificar las brechas de datos personales a la Agencia Española de Protección de Datos a excepción del caso de las Comunidades Autónomas de**[**Andalucía**](https://ws050.juntadeandalucia.es/vea/faces/vi/procedimientos.xhtml)**,**[**Cataluña**](https://apdcat.gencat.cat/es/inici/)**y**[**País Vasco**](https://www.avpd.euskadi.eus/s04-5273/es/contenidos/informacion/contacto/es_9493/es_contacto.html)**, cuando las brechas de datos personales se produzcan en entidades del sector público bajo su competencia.**

**Las notificaciones de brechas de datos personales a la AEPD se deben realizar de forma electrónica, usando el formulario de notificación de brechas de datos personales de la**[**Sede Electrónica**](https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/inicioEntidad.jsf)**para garantizar una correcta ejecución de las obligaciones del artículo 33.3 del RGPD.**

**La notificación a la autoridad de control de una brecha que afecta a datos personales forma parte de la responsabilidad proactiva establecida en el RGPD, y el hecho de notificarla no implica necesariamente la apertura de un procedimiento administrativo. De hecho, notificar en tiempo y forma es una evidencia de la diligencia de la organización, mientas que no cumplir con esa obligación si está tipificado como infracción.**

**Sin embargo, en aquellos casos en los que el responsable considere que no existieran riesgos para los derechos y libertades de las personas físicas el responsable tiene la obligación de documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el artículo 33 del RGPD.**

**Con el objetivo de ayudar en la obligación de notificar las brechas de datos personales a la autoridad de control, la AEPD ofrece indicaciones en la**[**Guía para la notificación de brechas de datos personales**](https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf)**así como otros recursos en el apartado de**[**innovación y tecnología**](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia#Brechas)**.**

**Comunicación de brechas de datos personales a los interesados**

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 34 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de comunicar a las personas afectadas aquellas brechas de datos personales que puedan entrañar un riesgo alto para sus derechos y libertades.

El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y en aquellos casos en los que determine que el riesgo para los derechos y libertades de las personas pueda ser alto, deberá comunicar la brecha a los afectados y [**notificarla a la autoridad de control competente**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion) conforme al artículo 33 del RGPD.

Con el objetivo de ayudar en la toma de decisiones, la AEPD ofrece la herramienta [**Comunica-Brecha RGPD**](https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd).

Consulte esta [**infografía**](https://www.aepd.es/es/documento/comunicar-brecha-datos-personales.pdf)para obtener más información sobre los requisitos para una buena comunicación a los afectados.

La comunicación a las personas afectadas debe realizarse en un lenguaje claro y sencillo, dirigirse específicamente a aquellas personas para las que exista un riesgo alto de que sus derechos y libertades pueden verse dañados, e incluir el siguiente contenido mínimo:

* **Datos de contacto del DPD, o en su caso, del punto de contacto en el que pueda obtenerse más información.**
* **Descripción general del incidente y momento en que se ha producido.**
* **Las posibles consecuencias de la brecha de datos personales.**
* **Descripción de los datos e información personal afectados.**
* **Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.**
* **Otras informaciones útiles para que los afectados puedan proteger sus datos o prevenir posibles daños.**

La comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

Cuando la comunicación a los afectados suponga un esfuerzo desproporcionado con relación a los riesgos para los derechos y libertades que están sufriendo los interesados, se podrá realizar una comunicación indirecta a través de avisos públicos.

En tal caso, el aviso público ocupará un lugar destacado, de forma que en ningún caso pueda pasar desapercibidos.

Una comunicación incompleta (sin el contenido mínimo), de difícil acceso o realizada a las personas incorrectas no es efectiva, por lo que una comunicación en estas condiciones podría llegar a considerarse una comunicación no realizada.

Con el objetivo de ayudar en la obligación de comunicar las brechas de datos personales a las personas afectadas, la AEPD ofrece indicaciones en la [**Guía para la notificación de brechas de datos personales**](https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf) así como otros recursos en el apartado de [**innovación y tecnología**](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia#Brechas).

# Códigos de conducta

Los códigos de conducta constituyen una muestra de lo que se denomina autorregulación, es decir, la capacidad de las entidades, instituciones y organizaciones para regularse a sí mismas.

En materia de protección de datos, son mecanismos de cumplimiento voluntario en los que se establecen reglas específicas para categorías de responsables o encargados del tratamiento con la finalidad de contribuir a la correcta aplicación del Reglamento general de protección de datos (RGPD) y la Ley Orgánica de protección de datos personales y garantía de los derechos digitales (LOPDPGDD).

El RGPD los configura como un instrumento del cumplimiento del principio de proactividad.

Los códigos de conducta pueden ser de alcance nacional, o transnacional si guardan relación con actividades de tratamiento en varios Estados miembros de la Unión Europea (UE).

## Normativa aplicable:

* [**RGPD**](https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807)**(arts. 40 y 41)**
* [**LOPDPGDD**](https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673)**(art. 38)**
* [**Directrices 1/2019 del Comité Europeo de Protección de Datos (CEPD)**](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_es.pdf)**en español**
* [**Directrices 1/2019 del Comité Europeo de Protección de Datos (CEPD)**](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf)**en inglés**
* [**Criterios de acreditación para los organismos de supervisión de códigos de conducta**](https://www.aepd.es/es/documento/acreditacion-organismos-supervision-cc.pdf)

### **Otra documentación de interés**

* [**Informe 0089/2020 del Gabinete Jurídico de la Agencia Española de Protección de Datos (AEPD)**](https://www.aepd.es/es/documento/2020-0089.pdf)

## Legitimación para promover un código de conducta:

Los códigos de conducta con arreglo al RGPD y la LOPDPGDD, que han de ser aprobados por la Agencia Española de Protección de Datos como autoridad de control competente, se podrán presentar por:

* **Asociaciones y otros organismos representativos de categorías de personas responsables y encargadas del tratamiento**
* **Empresas y grupos de empresas**
* **Los órganos, instituciones y entidades a los que se refiere el artículo 77.1 de la LOPDPGDD: Órganos constitucionales, AAPP, autoridades administrativas independientes, Universidades públicas, Fundaciones del sector público, consorcios…**
* **Organismos que asuman funciones de supervisión y resolución extrajudicial de conflictos**

## Contenido:

Su objeto es especificar la aplicación del RGPD en aspectos como:

* **El tratamiento leal y transparente**
* **Los intereses legítimos perseguidos por las personas responsables del tratamiento en contextos específicos**
* **La recogida de datos personales**
* **La seudonimización de datos personales**
* **La información proporcionada al público y a las personas interesadas**
* **El ejercicio de los derechos de las personas interesadas**
* **La información proporcionada a los menores de edad y la protección de éstos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el menor de edad**
* **Las medidas y procedimientos para garantizar la seguridad del tratamiento, así como la protección de datos desde el diseño y por defecto**
* **La notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a las personas interesadas**
* **La transferencia de datos personales a terceros países y organizaciones internacionales**
* **Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre las personas responsables del tratamiento y las personas interesadas relativos al tratamiento, sin perjuicio de los derechos de las personas interesadas**

No se establece un contenido obligatorio, pero éste debe responder a las necesidades específicas del sector o actividad de tratamiento de que se trate.

No obstante, los códigos de conducta deberán incluir obligatoriamente:

* **Los mecanismos para la supervisión de su cumplimiento**
* **Un organismo para la supervisión del cumplimiento del código que habrá de acreditarse por la Agencia Española de Protección de Datos (están exceptuados los códigos que regulen tratamientos efectuados por las entidades, instituciones y organismos a los que se refiere el artículo 77.1 de la LOPDPGDD)**

## Criterios de admisibilidad (Directrices 1/2019 CEPD)

Para facilitar una evaluación eficaz de cualquier proyecto de código, deberá incluir:

* **Una MEMORIA JUSTIFICATIVA clara y concisa, que describa detalladamente el objetivo del código, su ámbito de aplicación y cómo facilitará la aplicación efectiva del RGPD y, en su caso, documentación justificativa**
* **La justificación de la legitimación del promotor**
* **El ámbito de aplicación material que determine de forma clara y precisa las operaciones de tratamiento (o las características del tratamiento) de datos personales que abarca, así como las categorías de responsables o encargados del tratamiento a las que se aplica aportará soluciones prácticas**
* **El ámbito de aplicación territorial**
* **La autoridad competente, si se trata de códigos transnacionales**
* **Los mecanismos de supervisión**
* **El organismo de supervisión**
* **La consulta con las partes interesadas, o la justificación de su ausencia**
* **Y ser conformes con la legislación nacional**

## Criterios de aprobación de los códigos (Directrices 1/2019 CEPD)

Para su aprobación, los códigos deben demostrar que:

* **Satisfacen una necesidad específica del sector o actividad de tratamiento de que se trate**
* **Facilitan y especifican la aplicación de la normativa de protección de datos**
* **Aportan garantías suficientes**
* **Disponen de mecanismos suficientes para supervisar su cumplimiento**

## Incentivos de los códigos de conducta

En protección de datos los códigos de conducta sirven para adecuar y facilitar la aplicación del RGPD a las características de los distintos sectores de actividad de sus promotores y, además:

* **Pueden servir de elemento para demostrar el cumplimiento de las obligaciones de las personas responsables y encargadas**
* **Pueden servir de elemento para demostrar el cumplimiento de las obligaciones sobre medidas de seguridad (personas responsables y encargadas)**
* **Se tendrán en cuenta a efectos de evaluar el impacto en protección de datos de las operaciones de tratamiento –PIAS- (personas responsables y encargadas)**
* **Pueden servir de elemento para demostrar que la persona encargada adherida a un código ofrece garantías suficientes (personas encargadas o subencargadas)**
* **Pueden servir para aportar garantías suficientes para realizar transferencias internacionales de datos (en este caso su tramitación también requerirá el dictamen del CEPD)**
* **Se tendrán en cuenta en la determinación de sanciones**

## Códigos transnacionales

Cuando el código afecte a actividades de tratamiento en varios Estados miembros de la UE se deberá presentar ante la autoridad de control competente, para su determinación se tendrán en cuenta, entre otros, los siguientes criterios:

* **La ubicación de la mayor densidad del sector o de la actividad de tratamiento**
* **La ubicación de la mayor densidad de interesados afectados por el sector o actividad de tratamiento**
* **La ubicación de la sede del titular del código**
* **La ubicación del organismo de supervisión**
* **Las iniciativas desarrolladas por una autoridad de control en un ámbito específico**

## Organismos de supervisión

Los organismos de supervisión del cumplimiento de los códigos han de ser acreditados por la Agencia Española de Protección de Datos, para lo que tendrán que:

* **Demostrar independencia y experiencia en relación con el objeto del código**
* **Establecer procedimientos que le permitan evaluar la idoneidad de los responsables y los encargados del tratamiento correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y revisar periódicamente su aplicación**
* **Establecer procedimientos y estructuras para tramitar las reclamaciones sobre infracciones del código o la forma en que el código ha sido, o está siendo, aplicado por un responsable o encargado del tratamiento, y para hacer que dichos procedimientos y estructuras sean transparentes para los interesados y el público**
* **Demostrar de forma satisfactoria que sus funciones y deberes no dan lugar a un conflicto de intereses**

[**Registro de códigos de conducta nacionales**](https://www.aepd.es/es/informes-y-resoluciones/codigos-de-conducta)

[**Registro de códigos de conducta (Comité Europeo de Protección de Datos)**](https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en)

[**Listado de los códigos tipo inscritos anteriores al RGPD**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta/codigos-inscritos)

# Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales

**Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)**

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Los responsables y encargados del tratamiento podrán realizar transferencias internacionales de datos **SIN NECESIDAD DE AUTORIZACIÓN DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS** siempre que el tratamiento de datos observe lo dispuesto en el RGPD y en los siguientes supuestos:

## Transferencias basadas en una decisión de adecuación

Cuando las entidades receptoras de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea. Hasta la fecha los países y territorios están declarados como adecuados:

* [**Suiza. Decisión 2000/518/CE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0518&from=ES)**, de 26 de julio de 2000**
* [**Canadá. Decisión 2002/2/CE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002D0002&from=ES)**, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos**
* [**Argentina. Decisión 2003/490/CE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003D0490&from=ES)**, de 3 de junio de 2003**
* [**Guernsey. Decisión 2003/821/CE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003D0821&from=ES)**, de 21 de noviembre de 2003**
* [**Isla de Man. Decisión 2004/411/CE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32004D0411&from=ES)**, de 28 de abril de 2004**
* [**Jersey. Decisión 2008/393/CE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008D0393&from=ES)**, de 8 de mayo 2008**
* [**Islas Feroe. Decisión 2010/146/UE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010D0146&from=en)**, de 5 de marzo de 2010**
* [**Andorra. Decisión 2010/625/UE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010D0625&from=ES)**, de 19 de octubre de 2010**
* [**Israel. Decisión 2011/61/UE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011D0061&from=ES)**, de 31 de enero de 2011**
* [**Uruguay. Decisión 2012/484/UE, de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32012D0484&from=ES)**, de 21 de agosto de 2012**
* [**Nueva Zelanda. Decisión 2013/65/UE de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013D0065&from=ES)**, de 19 de diciembre de 2012**
* [**Japón. Decisión de 23 de enero de 2019**](http://europa.eu/rapid/press-release_IP-19-421_es.htm)
* [**Reino Unido. Decisión de 28 de junio de 2021**](https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf)**(versión en inglés)**
* [**República de Corea. Decisión de 17 de diciembre de 2021**](https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf)**(versión en inglés)**

El Tribunal de Justicia de la Unión Europea (TJUE) invalidó la [**Decisión (UE) 2016/1250 de la Comisión**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=es), de 12 de julio de 2016, conocida como el Escudo de Privacidad para las transferencias de datos a los estados Unidos. El Comité Europeo de Protección de Datos publicó las siguientes [**preguntas más frecuentes en relación con la sentencia**](https://www.aepd.es/es/documento/faqs-sentencia-schrems-ii-es.pdf) del TJUE.

## Mediante la aportación de garantías adecuadas

[**COMUNICADO DE LA AEPD - FINALIZACIÓN DEL PERÍODO PARA LA ADAPTACIÓN DE LOS CONTRATOS QUE UTILICEN LAS GARANTÍAS DE LAS CLÁUSULAS CONTRACTUALES TIPO DE LA COMISIÓN EUROPEA PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS**](https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales/comunicado-aepd)

A falta de decisión de adecuación si se ofrecen garantías adecuadas, que podrán ser aportadas a través de:

1. **Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos**
2. **Normas corporativas vinculantes**
3. **Cláusulas tipo de protección de datos adoptadas por la Comisión:  
   Con fecha 4 de junio de 2021, la Comisión Europea ha publicado el nuevo conjunto de cláusulas contractuales tipo que, además de sustituir a sus predecesoras, pretenden poder abarcar las transferencias entre responsables, entre responsable y encargado, entre encargados y entre encargado y responsable.  
   Las nuevas cláusulas se adaptan al RGPD incorporando los principios de responsabilidad proactiva y tratan de adoptar los criterios señalados por el Tribunal de Justicia de la Unión Europea (TJUE) en la sentencia del caso Schrems II. No obstante, sigue siendo necesario que el exportador de los datos, en su caso ayudado por el importador, analice el impacto que la legislación y/o la práctica vigente en el país del importador pueda tener en el nivel de protección proporcionado, de forma que sea esencialmente equivalente al que proporciona el marco europeo. Además, adicionalmente, deberán tenerse en cuenta las directrices del Comité Europeo de Protección de Datos sobre las medidas suplementarias que se considere adecuado adoptar para garantizar ese nivel de protección equivalente.  
   Las cláusulas contractuales de las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE quedan derogadas a partir del 27 de septiembre de 2021. No obstante, los contratos celebrados antes de dicha fecha con arreglo a las anteriores Decisiones serán válidos hasta el 27 de diciembre de 2022, siempre que las operaciones de tratamiento permanezcan inalteradas y las cláusulas contractuales garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas.**[**Decisión de Ejecución (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo**](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021D0914&qid=1623249029503&from=ES)
4. **Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión**
5. **Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas**
6. **Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.**

El Comité Europeo de Protección de Datos los siguientes documentos al respecto:

* [**Recomendaciones sobre medidas y garantías suplementarias a los instrumentos de transferencias para asegurar un nivel de protección sustancialmente equivalente al proporcionado en la Unión Europea**](https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf)**.**
* [**Recomendaciones sobre las garantías esenciales europeas para medidas de vigilancia**](https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_es.pdf)**.**
* [**Directrices relativas a las transferencias internacionales de datos entre autoridades y organismos públicos**](https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_es.pdf)**.**

## Excepciones para situaciones específicas

A falta de decisión de adecuación y de garantías adecuadas únicamente se podrán realizar si se cumple alguna de las condiciones siguientes:

1. **La persona interesada haya dado explícitamente su consentimiento, después de haber sido informada de los posibles riesgos**
2. **La transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada**
3. **La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica**
4. **La transferencia sea necesaria por razones importantes de interés público**
5. **La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones**
6. **La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento**
7. **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 sólo 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 resultase aplicable ninguna de estas excepciones, solo se podrá llevar a cabo una transferencia si no es repetitiva, afecta solo a un número limitado de personas interesadas, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades de la persona interesada, y el responsable del tratamiento evalué todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales.**

En este supuesto **el responsable del tratamiento informará a la autoridad de control de la transferencia**. Además de la información a que hacen referencia los artículos 13 y 14 del RGPD, el responsable del tratamiento informará a la persona interesada de la transferencia y de los intereses legítimos imperiosos perseguidos.

El Comité Europeo de Protección de Datos ha elaborado unas [**Directrices sobre la aplicación de las excepciones**](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf).

## ¿Cuándo se necesita una autorización expresa de la Agencia Española de Protección de Datos?

Cuando el ofrecimiento de garantías adecuadas se realice mediante:

1. **Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o subencargado, que no hayan sido adoptadas por la Comisión Europea o por la Agencia Española de Protección de Datos y aprobadas por la Comisión Europea**
2. **Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para las personas interesadas**

Autorizaciones para la transferencia internacional de datos aprobadas por la AEPD en el marco del RGPD: [**TI-00001-2019-Resolución Autorización Comisión Nacional del Mercado de Valores (CNMV) – 14-05-2019**](https://www.aepd.es/es/documento/ti-00001-2019-resolucion-autorizacion-cnmv.pdf)

## Normas Corporativas Vinculantes (BCR)

Las normas corporativas vinculantes (o BCR -Binding Corporate Rules- por sus siglas en inglés) son “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”.

Los grupos empresariales son aquellos “constituidos por una empresa que ejerce el control y sus empresas controladas”.

Las normas corporativas vinculantes deberán cumplir los requisitos y contenidos establecidos en el artículo 47 del RGPD.

La autoridad de control competente las aprobará de conformidad con el mecanismo de coherencia establecido en el artículo 63 del RGPD. La autoridad de control competente se determinará con arreglo a criterios como:

* **La ubicación de la sede europea del grupo empresarial**
* **La ubicación de la compañía del grupo empresarial que tenga la responsabilidad en protección de datos**
* **La ubicación de la compañía del grupo mejor situada (en términos de gestión, carga administrativa) para tramitar la solicitud y obligar al cumplimiento de las normas corporativas vinculantes**
* **Donde se tomen la mayoría de las decisiones sobre los fines y medios del tratamiento de datos, como las transferencias**
* **El Estado miembro de la Unión Europea desde el que se realizan la mayoría de las transferencias internacionales**

Los grupos empresariales interesados en la elaboración de normas corporativas vinculantes pueden solicitar información en la siguiente dirección de correo electrónico: [**sgpromocion.autorizaciones@aepd.es**](mailto:sgpromocion.autorizaciones@aepd.es).

### **Normas corporativas vinculantes aprobadas por la AEPD:**

**GRUPO FUJIKURA AUTOMOTIVE EUROPE**

* [**Resolución de aprobación de las normas corporativas vinculantes de responsable (BCR-C) del grupo FUJIKURA AUTOMOTIVE EUROPE (GRUPO FAE)**](https://www.aepd.es/es/documento/ti-00001-2020-resolucion-aprobacion-bcr-fae.pdf)
* [**Enlace a las normas corporativas vinculantes (BCR-C) del grupo FAE**](http://www.fujikura-automotive.com/sites/default/files/documents/BCR.pdf)

**GRUPO IBERDROLA**

* [**Resolución de aprobación de las normas corporativas vinculantes de responsable (BCR-C) del grupo IBERDROLA**](https://www.aepd.es/es/documento/ti-00002-2020-resolucion-aprobacion-bcr-iberdrola.pdf)
* [**Enlace a las normas corporativas vinculantes (BCR-C) del grupo IBERDROLA**](https://www.iberdrola.com/politica-privacidad/normas-corporativas-vinculantes)

**GRUPO KUMON**

* [**Resolución de aprobación de las normas corporativas vinculantes de responsable (BCR-C) del grupo KUMON**](https://www.aepd.es/es/documento/ti-00001-2021-resolucion-aprobacion-bcr-r-kumon.pdf)
* [**Enlace a las normas corporativas vinculantes (BCR-C) del grupo KUMON**](https://www.kumon.ne.jp/bcr/img/BCRs_Controller_Policy_Spanish.pdf)

**GRUPO KUMON**

* [**Resolución de aprobación de las normas corporativas vinculantes de encargado (BCR-P) del grupo KUMON**](https://www.aepd.es/es/documento/ti-00002-2021-resolucion-aprobacion-bcr-e-kumon.pdf)
* [**Enlace a las normas corporativas vinculantes (BCR-P) del grupo KUMON**](https://www.kumon.ne.jp/bcr/img/BCRs_Processor_Policy_Spanish.pdf)

**AMERICAN EXPRESS**

* [**Enlace a las normas corporativas vinculantes de responsable (BCR-C) de American Express**](https://www.americanexpress.com/es-es/empresa/legal/centro-de-privacidad/normas-corporativas-vinculantes/)

**GRUPO COLT**

* [**Resolución de aprobación de las normas corporativas vinculantes de responsable (BCR-C) del grupo COLT**](https://www.aepd.es/es/documento/ti-00003-2021-resolucion-aprobacion-bcr-responsable-colt.pdf)
* [**Enlace a la información relativa a las normas corporativas vinculantes del grupo COLT**](https://www.colt.net/legal/data-privacy/#bcr)

**GRUPO COLT**

* [**Resolución de aprobación de las normas corporativas vinculantes de encargado (BCR-P) del grupo COLT**](https://www.aepd.es/es/documento/ti-00004-2021-resolucion-aprobacion-bcr-encargado-colt.pdf)
* [**Enlace a la información relativa a las normas corporativas vinculantes del grupo COLT**](https://www.colt.net/legal/data-privacy/#bcr)

**GRUPO ANTOLIN**

* [**Resolución de aprobación de las normas corporativas vinculantes de responsable (BCR-C) del grupo ANTOLIN**](https://www.aepd.es/es/documento/ti-00001-2022-resolucion-aprobacion-bcr-antolin.pdf)
  + [**Enlace a la información relativa a las normas corporativas vinculantes del grupo ANTOLÍN**](https://www.grupoantolin.com/es/politica-privacidad)

**Enlaces a los documentos más relevantes para la elaboración de unas BCR**

[**Recomendaciones 1/2022: solicitud, elementos y principios para la elaboración de BCR de responsable**](https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplicationform_en.pdf)

[**Modelo de solicitud de BCR de encargados**](https://www.aepd.es/es/documento/wp195a_en-1.doc)

[**Procedimiento para la aprobación de BCR de responsables y encargados**](https://www.aepd.es/es/documento/wp263_en.pdf)

[**Elementos y principios BCR de encargados**](https://www.aepd.es/es/documento/wp257_en.pdf)

# Directrices de aplicación

[**Pequeñas y Medianas Empresas (PyMES)**](https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/directrices-de-aplicacion/pymes)

[**Administraciones Públicas**](https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/directrices-de-aplicacion/administraciones-publicas)

[**Directrices de las personas delegadas de protección de datos**](https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf)

[**Directrices sobre el derecho a la portabilidad de datos**](https://www.aepd.es/sites/default/files/2019-09/wp242rev01-es.pdf)

[**Directrices sobre criterios de identificación de la “autoridad líder”**](https://www.aepd.es/sites/default/files/2019-12/wp244rev01-es.pdf)

[**Directrices sobre Evaluación de Evaluación de Impacto (EIPD) y para determinar que el tratamiento suponga un alto riesgo**](https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es_0.pdf)

[**Directrices sobre notificación de las brechas de seguridad de los datos personales (Documento pendiente de consulta pública)**](https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf)

[**Directrices sobre decisiones individuales automatizadas y perfilado a efectos del RGPD**](https://www.aepd.es/sites/default/files/2019-12/wp251rev01-en.pdf)

[**Dictamen sobre el concepto de interés legítimo**](https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf)