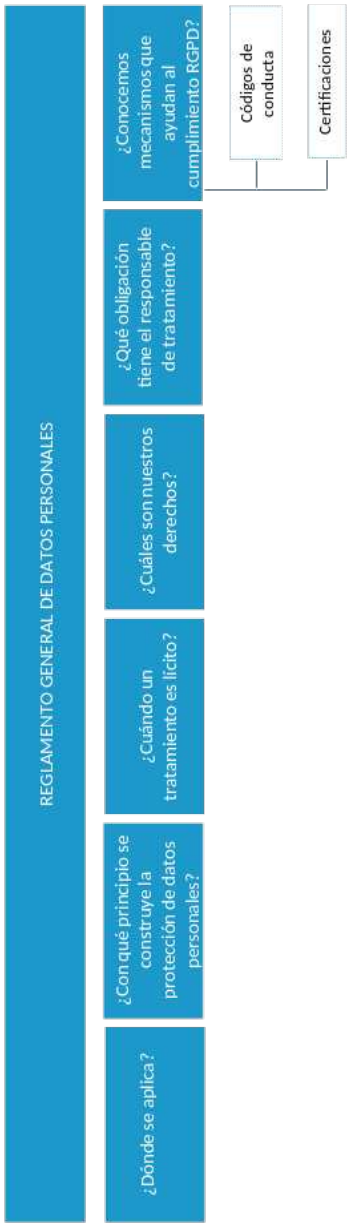
Gobierno del Dato y Toma de Decisiones

Tema 8. Introducción a la protección de datos

Índice

Esquema



8.1. Introducción y objetivos

Este tema desarrolla los principios de la protección de datos de carácter personal, y para ello nos introducimos en el marco internacional más exigente, que es el de la UE. Este marco se aplica a los países miembros de la UE y está influyendo notablemente en el desarrollo normativo de otros países fuera del espacio europeo. Además, extiende su aplicación fuera de las fronteras de la UE.

Para lograr soltura en la lectura de textos legales, aconsejamos consultar la información disponible en la web de la Agencia Española de Protección de Datos (AEPD) sobre 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), en adelante RGPD.

8.2. Conceptos

Las diferentes legislaciones en materia de privacidad y protección de datos de carácter personal tienen por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Es importante entender los conceptos aquí incorporados para seguir adecuadamente el contenido de la asignatura.

Principales conceptos (art. 4, RGPD)

- «"Datos personales": toda información sobre una persona física identificada o identificable (el interesado)» (art. 4.1, RGPD).

Y se considerará **persona física identificable** «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (art. 4.1, RGPD).

Un aspecto controvertido por su carácter interpretativo se deriva del término *identificable,* es decir, información que facilita de manera indirecta identificar a una persona. Este sería el caso de, por ejemplo: la dirección IP, el número de teléfono fijo, la cadena de ADN, la huella dactilar, datos biométricos, etc. Para entender mejor el concepto de identificable, podemos recurrir al considerando 26 RGPD, que explica que la determinación de si una persona física es identificable, se han de tener en consideración todos los medios, razonablemente accesibles por «alguien» que

permitan identificar de una forma bien sea directa o indirecta (a través de algún identificador) a la persona física. Se deben tener en consideración todos los medios técnicos disponibles, los costes operativos y económicos asociados y el tiempo requerido para considerar la probabilidad de que dicha identificación sea posible. Una cuestión que habrá que tener en cuenta en ámbitos de aplicaciones móviles o IoT que, a través de identificadores únicos asociados a dispositivos o una *app,* estos pueden permitir la identificación inequívoca.

- «"Tratamiento": cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (art. 4.2, RGPD).

- «"Limitación del tratamiento": el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro» (art. 4.3, RGPD).

- «"Elaboración de perfiles": toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física» (art. 4.4, RGPD).

- «"Pseudonimización": el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable» (art. 4.5, RGPD).

Ideas clave

- «“Fichero”: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica» (art. 4.6, RGPD).
- «“Responsable del tratamiento” o “responsable”: la persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento» (art. 4.7, RGPD).
- «“Encargado del tratamiento” o “encargado”: la persona física o jurídica, autoridad, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento» (art. 4.8, RGPD).
- «“Destinatario”: la persona física o jurídica, autoridad, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento» (art. 4.9, RGPD).
- «“Tercero”: persona física o jurídica, autoridad, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado» (art. 4.10, RGPD).
- «“Consentimiento del interesado”: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen» (art. 4.11, RGPD).

Ideas clave

- «“Violación de la seguridad de los datos personales”: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (art. 4.12, RGPD). La violación también puede ser referida como **brecha de seguridad.**

- «“Datos genéticos”: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona» (art. 4.13, RGPD).

- «“Datos biométricos”: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos» (art. 4.14, RGPD). Los datos biométricos tienen un uso creciente en métodos de autenticación de las personas. El RGPD permite a los estados miembros legislar sobre las condiciones adicionales o limitaciones del tratamiento de datos biométricos, genéticos o relativos a la salud (art. 9.4, RGPD).

- «“Datos relativos a la salud”: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud» (art. 4.15, RGPD). Los datos de salud disponen de un marco de amparo garantista específico por las características y el impacto que dichos datos tienen en los ciudadanos, de ahí que exista una definición específica al respecto.

Ideas clave

- «“Establecimiento principal”:

  - »En lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal.

  - »En lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento» (art. 4.16, RGPD).

- «“Representante”: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento» (art. 4.17, RGPD).

- «“Empresa”: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica» (art. 4.18, RGPD).

- «“Grupo empresarial”: grupo constituido por una empresa que ejerce el control y sus empresas controladas» (art. 4.19, RGPD).

Ideas clave

- «“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» (art. 4.20, RGPD). Las reglas corporativas vinculantes BRC (acrónimo en inglés) se configuraron en su momento como vehículo para racionalizar las transferencias internacionales de datos en grupos corporativos siempre con la autorización de la autoridad competente.

- «“Autoridad de control”: la autoridad independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51» (art. 4.21, RGPD). En términos genéricos, hablamos de agencias de protección de datos de los Estados miembros. En el caso de España, la autoridad es la Agencia Española de Protección de Datos.

- «“Autoridad de control interesada”: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

  - »El responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control.

  - »Los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento.

  - »Se ha presentado una reclamación ante esa autoridad de control» (art. 4.22, RGPD).

Es de resaltar la posibilidad de presentar reclamaciones, por parte de los afectados, a las autoridades de control de su país de residencia, aunque el tratamiento tenga lugar en otro estado miembro.

- «Tratamiento transfronterizo»: se establece en dos circunstancias diferenciadas:

  - «El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro.

  - »El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro» (art. 4.23, RGPD).

Estaremos ante un tratamiento transfronterizo siempre que los datos crucen la frontera, bien porque el responsable del tratamiento o encargado está presente en diferentes Estados de la UE, bien porque afecta a ciudadanos residentes en Estados diferentes al de residencia del responsable o encargado de tratamiento.

- «“Objeción pertinente y motivada”: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión» (art. 4.24, RGPD).

Ideas clave

- «“Servicio de la sociedad de la información”: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo» (art. 4.25, RGPD). Es decir, todo servicio de la sociedad de la información o todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

- «“Organización internacional”: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo». (art. 4.26, RGPD).

8.3. Principios generales de protección de datos en Europa

El RGPD se construye sobre siete principios generales, un conjunto de reglas básicas y de obligado cumplimiento, para el tratamiento de datos de carácter personal. El RGPD consolida y amplia los principios existentes en la legislación europea anterior (la directiva 95/40/CE) (art. 5., RGPD).

Figura 1. Principios de la protección de datos personales RGPD. Fuente: elaboración propia.

Ideas clave

- **Licitud, lealtad y transparencia.** Los datos de carácter personal deben ser tratados de manera:
  - **Lícita** (art. 6, RGPD).
  - **Leal:** «fidedigno, verídico y fiel, en el trato o en el desempeño de un oficio o cargo» (RAE, 2020).
  - **Transparente** (art. 12, RGPD).

Es decir, el tratamiento debe ser conforme a la Ley, tal y como se establece la legitimidad en el RGPD, debe ser fiel por parte de los responsables de tratamiento frente a los afectados, no debe mediar engaño ni tratar los datos sin lealtad al consentimiento obtenido por parte del afectado. Y debe permitir al afectado conocimiento sobre el tratamiento al que están sometidos sus datos personales., en los términos que refleja el RGPD, que veremos más adelante.

Ideas clave

- **Limitación de la finalidad.** Recabados para una finalidad concreta, que debe ser explícita y legítima, de manera que los datos no podrán ser tratados posteriormente para ninguna otra finalidad, a menos que la nueva finalidad tenga la consideración de compatible, como es el caso del tratamiento de datos para fines posteriores como son los casos de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. «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 considerará incompatible con los fines iniciales ("limitación de la finalidad")» (art. 5.1, RGPD).

  El tratamiento de datos con finalidades históricas, científicas y estadísticas deben **realizarse conforme a las garantías establecidas en el propio RGPD.** El artículo 89 («Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos») fija, entre otras, la necesidad de incorporar al tratamiento medidas técnicas y organizativas, garantizar el respeto al principio de minimización de los datos personales y aplicar si es posible pseudonimización.

- **Minimización de datos.** Los datos recabados deben ser adecuados, pertinentes y limitados a los estrictamente necesarios para la finalidad prevista para la que son recabados.

  Esto implica que **la finalidad ha de justificar los datos que están siendo objeto de tratamiento,** de manera que la misma finalidad no pueda satisfacerse con un conjunto de datos de los afectos menor.

- **Exactitud de los datos.** Los datos deberán ser exactos y estar actualizados, y el responsable de tratamiento debe tomar las medidas necesarias para que los datos que sean inexactos con respecto a los fines del tratamiento se supriman o rectifiquen sin retrasos.

Ideas clave

- **Limitación del plazo de conservación.** Los datos personales se mantendrán, permitiendo la identificación de los afectados, por el tiempo estrictamente necesario para los fines del tratamiento. Solo podrán conservarse si se tratan exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siempre que sea conforme al artículo 89, apartado 1, del RGPD. En cualquier caso, el responsable de tratamiento debe aplicar las medidas técnicas y organizativas necesarias establecidas en el RGPD para proteger los derechos y libertades del interesado.

- **Seguridad adecuada: confidencialidad e integridad.** Los datos serán tratados de manera que se garantice la seguridad adecuada, que debe incluir la protección frente al tratamiento no autorizado o ilícito, su pérdida, destrucción o el daño accidental. Para ello deberá aplicar las medidas técnicas y organizativas apropiadas.

- **Responsabilidad proactiva.** El responsable del tratamiento debe velar en todo momento por la licitud, lealtad y la trasparencia del tratamiento y el cumplimiento de los principios establecidos.

El principio de la responsabilidad proactiva (art. 5.2, RGPD) establece la obligación de los responsables de tratamiento (RT), de actuar con diligencia, de forma proactiva y continuada, para garantizar el cumplimiento del Reglamento General de Protección de Datos, y de este modo garantizar los derechos y libertades de los afectados.

Por ejemplo:

- Debe ser el responsable del tratamiento quien pruebe la legitimidad del tratamiento, mediante prueba de haber obtenido el consentimiento del afectado o en aplicación de otros principios de legitimación.
- Debe ser el responsable del tratamiento (RT) quien, ante una situación de violación de la seguridad, deba demostrar la improbabilidad de que dicha violación entrañe riesgo para los derechos y libertades de las personas físicas.

Exigir esta responsabilidad tiene por objeto garantizar los derechos de los afectados (considerando 85, RGPD).

Ámbito de aplicación

El ámbito de aplicación de la legislación no diferencia los sistemas de tratamiento utilizados en el tratamiento de datos de carácter personal.

El RGPD es aplicable a los tratamientos independientemente de que estos sean automatizados, manuales o mixtos (art. 2, RGPD).

Pero no se aplica a todos los tratamientos de datos de carácter personal, existen exclusiones.

El RGPD no será de a aplicación a los tratamientos efectuados por los ciudadanos, en el ámbito de su vida personal y doméstica.

Tampoco se aplicará en los tratamientos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención (art. 2, RGPD); así como los derivados de la aplicación del capítulo 2 del título V del TUE (Tratado de la UE), que aborda las políticas sobre controles en las fronteras, asilo e inmigración.

Referente la aplicación geográfica, **la norma se aplicará a los responsables de tratamiento que se encuadren fuera de la UE** en alguno de los supuestos siguientes (art. 3, RGPD):

- Si el tratamiento se realiza en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de dónde se realiza el tratamiento y dónde reside el afectado, el tratamiento estará sometido al RGPD (art. 3.1, RGPD).

- Si el tratamiento se realiza por parte de responsables de tratamiento residentes fuera de la UE, que o bien ofrecen bienes o servicios a residentes europeos o realizan prácticas de control o seguimiento de su comportamiento (art. 3.2, RGPD).

Hay que recordar que en este segundo caso el responsable de tratamiento o el encargado deberá asignar un representante en la UE, a menos que sea el tratamiento ocasional y de bajo riesgo para los derechos libertados de los afectados porque, por ejemplo, no afecta a categorías de datos especiales como salud, origen racial, etc. (art. 27, RGPD).

Situaciones a las que se añadirán aquellas en las que el derecho de los Estados miembros se aplique en virtud del derecho internacional público como, por ejemplo, las embajadas.

De modo que la aplicación del RGPD transciende el espacio de la UE al establecer como hecho objetivo circunstancias que solo dependen de que el tratamiento se realice sobre ciudadanos residentes en la UE y no sobre la residencia del responsable de tratamiento o encargado del mismo.

Extiende el ámbito de aplicación territorial a entidades no radicadas en la UE con actividades que se centren en la oferta de bienes o servicios dirigidas a ciudadanos residentes en la Unión Europea o al seguimiento de estos. Por ejemplo, páginas web de noticias, de venta de servicios o productos dirigidos al espacio de la UE.

Veamos un esquema de decisión sobre cuándo el responsable de tratamiento debe quedar regulado por el Reglamento General de Protección de Datos.

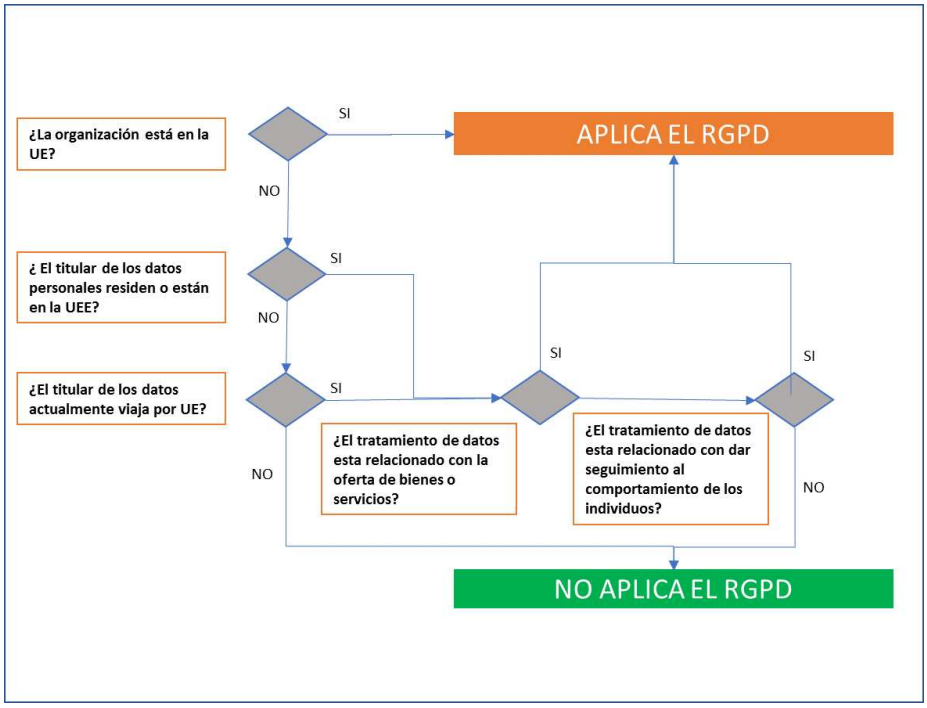


Figura 2. Diagrama de flujo para aplicar RGPD.

8.4. Licitud de tratamiento. El consentimiento informado

El RGPD establece bajo qué circunstancias el tratamiento tendrá la consideración de lícito, siendo responsabilidad del responsable de tratamiento que el mismo se ampare en dichas circunstancias. (art .6, RGPD).

El tratamiento será lícito, como principio general si existe consentimiento por parte del interesado. El interesado facilitó el consentimiento del tratamiento de sus datos para el fin o finalidades requeridos (art. 6.1, RGPD).

Pero existen otras circunstancias para las que no es indispensable el consentimiento del interesado, al cumplir alguna de las siguientes condiciones (art. 6.1, RGPD):

- El tratamiento es necesario para la ejecución de un contrato por parte del interesado.
- El tratamiento es **necesario para dar cumplimiento a una obligación legal** del responsable de tratamiento. Por ejemplo, esta condición da amparo al tratamiento que realizan las empresas en relación con el cumplimiento de sus obligaciones de la legislación laboral.
- El tratamiento está destinado y **es necesario para proteger un interés vital** del propio interesado o de otra persona. Como es el caso de situaciones de vida o muerte del afectado.
- Si el tratamiento es necesario **para el cumplimiento de una misión pública** o en ejercicio de poderes públicos. Un ejemplo es la publicación de listados de colegiados por parte de los colegios profesionales, en cumplimiento de su misión de ordenación de la actividad de los colegiados y obligación de publicidad para velar por los intereses de los usuarios.

Ideas clave

- **El tratamiento es necesario para la satisfacción de intereses legítimos** perseguidos por el responsable del tratamiento o una tercera parte.

Hay situaciones en las que el responsable de tratamiento puede hacer valer su interés legítimo a la hora de efectuar un tratamiento de datos personales, sin necesidad de que exista consentimiento del afectado, siempre que no prevalezca este interés legítimo frente a los derechos de los afectados y no afecte a categorías especiales de datos.

Para entender un poco mejor de qué situaciones estamos hablando, nada mejor que recurrir al texto del RGPD, concretamente al considerando 47:

> «El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin» (considerando 47, RGPD).

El propio considerando nos da dos ejemplos de tratamientos bajo interés legítimo: «el tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude [y] el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo» (considerando 47, RGPD).

Para profundizar en esta cuestión está disponible el Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, del Grupo de trabajo del artículo 29, del año 2014: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

Por último, hay que destacar que el RGPD prevé que los estados miembros puedan introducir disposiciones que amplíen o concreten los aspectos recabados en los apartados b) y d).

Tratamiento de datos de menores de edad y su consentimiento

El tratamiento de datos de menores tiene una consideración especial, por su vulnerabilidad, como en estos casos (considerando 38, RGPD):

- Utilización de datos personales de niños con fines de mercadotecnia.
- Elaboración de perfiles de personalidad o de usuario.
- Obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño.

Para ello la norma establece que el consentimiento del menor solo sea válido a partir de los 16 años (art. 8, RGPD). Ahora bien, la norma reconoce el hecho diferencial y de costumbre de los países de la UE que no atribuyen a la misma edad la capacidad de obrar en su propio nombre, por ello el RGPD reconoce a los Estados miembros de la UE la capacidad de poder determinar la edad a partir de la cual se considera con capacidad de consentir, que no podrá ser menor de 13 años. Así, en España, la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) fija la edad válida para el consentimiento en los 14 años.

Para el tratamiento de los datos de los menores de 14 años que se fundamente en el consentimiento, será necesario recoger el consentimiento titular de la patria potestad o tutela del menor. El responsable de tratamiento deberá demostrar que cuenta con este consentimiento.

Para los menores de edad, el consentimiento al tratamiento de datos personales debe ser facilitado por los padres o tutores.

Aunque también contempla limitaciones (considerando 38, RGPD) y no debe requerirse en el acceso o utilización de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños. Un ejemplo: servicios de prevención de maltrato infantil o acoso escolar.

Tratamiento de datos de categorías especiales

El RGPD en su artículo 9 prohíbe de manera taxativa el tratamiento de datos personales considerados especiales. Las categorías de datos especiales son:

- Los datos que revelen el origen étnico o racial.
- Las opiniones políticas.
- Las convicciones religiosas.
- Las convicciones filosóficas.
- La afiliación sindical.
- Los tratamientos de datos genéticos.
- Los datos biométricos dirigidos que identifican unívocamente a una persona.
- Los datos relativos a la salud de las personas.
- Los datos relativos a la vida sexual de las personas o a su orientación sexual.

Ideas clave

Será legítimo el tratamiento de los datos correspondientes a categorías especiales cuando medie **consentimiento explícito** por parte del afectado o se den alguna de las siguientes circunstancias:

- Se requiere para que el responsable del tratamiento cumpla con sus obligaciones legales en el marco laboral y de la seguridad social.
- Es necesario para proteger un interés vital del afectado o de otra persona, si el afectado no está en disposición de otorgar su consentimiento, por ejemplo, por estar incapacitado físicamente.
- El tratamiento es realizado en el marco de la actividad de una organización sin ánimo de lucro, fundación o asociación cuya finalidad sea política, filosófica, religiosa o sindical. Esta excepción solo es aplicable para el caso de que los afectados sean miembros o lo hubieran sido o se trate de simpatizantes que se comuniquen con frecuencia. Todo ello siempre que el tratamiento sea dentro de la organización y cualquier comunicación al exterior requerirá consentimiento del afectado.
- Los datos son públicos y ha sido el interesado el que los ha hecho públicos.
- Cuando el tratamiento sea necesario en las acciones de reclamaciones judiciales.
- El tratamiento es necesario por razones de interés público, avalado por la ley.
- El tratamiento es necesario en el ámbito de la asistencia sanitaria o medicina preventiva conforme al derecho de la UE.
- El tratamiento es necesario por motivos de salud pública conforme al derecho de la UE.
- El tratamiento es necesario para fines de archivo de interés público, histórico, científico o estadístico conforme al derecho de la UE.

8.5. Derecho de información

El RGPD establece la obligación de que el responsable de tratamiento, cuando vaya a recabar datos personales y de manera previa a su recogida o su registro, deba informar a los interesados. Este derecho se desarrolla en el RGPD en dos artículos:

- Artículo 13: «Información que deberá facilitarse cuando los datos personales se obtengan del interesado».
- Artículo 14: «Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado».

El **objetivo** es:

- **Garantizar la transparencia** del tratamiento de manera que se conozca claramente la finalidad del tratamiento, quien va a efectuar el mismo y el tiempo durante el cual los datos serán tratados.
- **Sustentar la legitimidad del tratamiento** cuando este se base en el consentimiento del afectado, basado en la información facilitada por el responsable de tratamiento.
- **Informar de los derechos que asiste al afectado** con respecto al tratamiento de datos personales y dónde poder ejercitarlo, facilitando información de la empresa y datos de contacto.
- **Conocer si los datos serán exportados internacionalmente,** identificando los países destinatarios y la existencia de un nivel de protección equivalente al europeo.

Ideas clave

Cuando los datos se recaban directamente del interesado, por ejemplo, en los casos en que los datos proceden de alguna comunicación o cesión legitima, la organización receptora de los datos debe informar a los interesados en un plazo razonable (art. 14.2, RGPD):

- Como máximo antes de que trascurra un mes desde que se consiguen los datos.
- En el caso de que los datos personales sean para comunicarse con el interesado, se deberá informar como tarde en la primera comunicación con el interesado (por ejemplo, en el primer envío de información publicitaria).
- Y habrá que informar antes de que los datos se comuniquen a terceros, otros destinatarios.

El responsable de tratamiento debe actuar proactivamente, garantizando el derecho de información antes de la recogida de los datos, y debe probar que cumplió con la obligación de informar.

Hay excepciones a esta obligación: por un lado, cuando ya el interesado disponga de dicha información; por otro, siendo los datos no recabados directamente del interesado (datos cedidos o comunicados por un tercero), cuando se de alguna de las siguientes circunstancias (art. 14.5, RGPD):

- La comunicación no sea posible o suponga un esfuerzo desproporcionado, por ejemplo, en situaciones de un volumen desproporcionado de usuarios y en particular cuando el tratamiento tenga fines de archivo en interés público, investigación científica o histórica o fines estadísticos.
- La obtención de los datos o la obligación de su comunicación esté recogida en el ordenamiento jurídico.
- Cuando por ley el tratamiento de los datos deba tener carácter confidencial.

Ideas clave

Tal y como recoge el artículo 12 («Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado»):

> «La información facilitada, dentro del marco de transparencia, debe ser clara, concisa, transparente, legible de fácil compresión» (art. 12, RGPD).

En especial, en los casos en los que la información se dirija a los niños. En la práctica, nos encontramos con formas habituales de informar como son los típicos formularios en papel o electrónicos de registro de usuarios, pero también van creciendo otros puntos de recogida de datos, lo que implica establecer nuevos mecanismos para garantizar el derecho de información. Por ejemplo, se recopilan datos en aplicaciones móviles, mediante sensores IoT, durante la navegación de páginas web, en entrevistas telefónicas, etc.

En cualquiera de los casos, siempre habremos de aplicar el principio de transparencia y la capacidad de demostrar el cumplimiento del derecho de información.

El RGPD contempla dos posibles situaciones a la hora de informar, que no solo afectan al momento en el que se ha de facilitar la información, sino también a la información misma por facilitar. Así tenemos:

1. Los datos se recaban directamente del interesado (artículo 13).
2. Los datos no se obtienen directamente del interesado (artículo 14).

Ideas clave

A continuación, veremos los requerimientos de información concretos para cada uno de los casos.

- Los datos se recaban directamente del interesado. En este caso la información que debe ser facilitada al interesado es (art. 13, RGPD):
- La identificación de quien determina la finalidad del tratamiento de los datos:
  - La identidad del responsable del tratamiento y los datos de contacto y, en su caso, de su representante.
  - Los datos de contacto del delegado de protección de datos.
- Para qué se van a tratar los datos: finalidad del tratamiento.
- La base de legitimación del tratamiento:
  - El consentimiento explícito del afectado.
  - O la base jurídica del mismo, cuando para el tratamiento no se requiere que exista consentimiento por parte del interesado por la legislación.
  - O los intereses legítimos explícitos, del responsable del tratamiento, cuando el tratamiento se legitimase en ellos.
- Los destinatarios de los datos personales, que no necesariamente debe ser solo el responsable de tratamiento.
- Sobre las transferencias internacionales:
  - Informar de la transferencia prevista, países destinatarios.
  - Indicar si existe o no el reconocimiento de adecuación por parte de la Comisión Europea.

Ideas clave

- El plazo de conservación de los datos:
  - El tiempo de conservación establecido.
  - Criterios que determinarán el plazo de conservación.
- Los derechos del afectado:
  - Acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad de los datos.
  - Derecho a retirar el consentimiento, para el caso de que el tratamiento se legitimase en virtud del consentimiento del afectado, sin que ello afecte al tratamiento realizado previamente.
  - Derecho a presentar reclamación frente a la autoridad de control.
- Sobre la obligación de facilitar los datos o de las consecuencias de no facilitarlos, indicando si los datos obligatorios se han de facilitar por:
  - Requisito legal o contractual.
  - Requisito para suscripción de un contrato.
- Si los datos serán utilizados para la toma de decisiones automatizadas o elaboración de perfiles, deberá informar:
  - Explicación razonable de la lógica aplicada.
  - Y las consecuencias previstas del tratamiento para el interesado.
- Los datos no se recaban directamente del interesado. En este caso, a la información anteriormente especificada habrá que añadir (art. 14, RGPD):
- El origen de los datos.
- Las categorías de datos personales que son objeto de tratamiento.

Debemos tener en consideración que, al no ser los datos recabados directamente del interesado, el interesado no dispone de esta información.

El RGPD recoge la **posibilidad de que la información sea facilitada por capas o niveles.** De manera que se disponga de una **primera capa con información básica resumida** que se presentaría al afectado en el mismo momento y en el mismo medio utilizado para la recogida de los datos. También se incluiría una referencia mediante la que se redirige al usuario para acceder a una segunda capa de información adicional, donde se ha incorporado de forma detallada toda la información requerida.

Por ejemplo, la Agencia Española de Protección de Datos, para el ejercicio del derecho a la información, recomienda el siguiente esquema de agrupación de la información por capa a modo de resumen:

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

Figura 3. Esquema de agrupación de la información. Fuente: AEPD, s.f.

El RGPD posibilita que la información que se facilita en la primera capa se articule en torno a la combinación de iconos normalizados. Se pretende facilitar de un modo sencillo, fácilmente visible y legible una primera información sobre las características del tratamiento. Información que será ampliable conforme a lo anteriormente expuesto.

De esta manera, se trata de dar respuesta al habitual desistimiento por parte de los interesados de la lectura de cláusulas informativas y la tendencia a otorgar el consentimiento sin reparar en la información del tratamiento al que se está consintiendo. De este modo, unos iconos facilitan una primera aproximación que, aunque no exhaustiva, sí sirve al usuario para focalizar la atención e incluso diferenciar unos escenarios de otros de forma sencilla y visual. Por ejemplo, si existen cesiones o comunicaciones de datos o si los datos serán objeto de transferencia internacional. El establecimiento de este conjunto normalizado de iconos es potestad de la Comisión Europea.

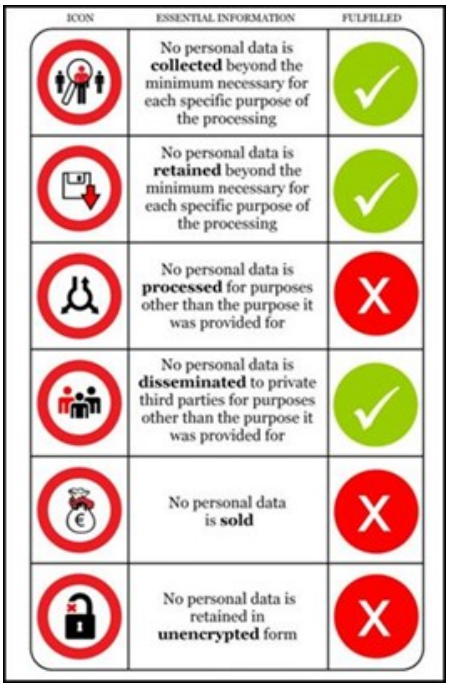


Figura 4. Ejemplo de los iconos propuestos en la fase legislativa del RGPD. Fuente: Hoskins, 2012.

Ejemplo de cláusula de información para el cumplimiento con el derecho de información

- Información básica (primera capa):

Responsable	Editorial de publicidad S. A.
Finalidad	Gestión de la suscripción a la publicación semanal de la revista.
Legitimación	Ejecución de un contrato.
Destinatarios	No se contemplan cesiones más que las legalmente exigidas.
Derechos	Acceder, rectificar y suprimir los datos, para conocer todos sus derechos; acceder a la información adicional.
Información adicional	Puede consultar la información adicional en detalle en relación con el tratamiento de datos de carácter personal en la página web http://www.edipublisa.com/IRGPD (link simulado para el ejemplo).

- Información adicional (segunda capa):

Responsable del tratamiento

Identidad: Editorial de publicidad S. A. CIF: A99855669.

Dirección: C/LOPD n.o 22, Madrid, 28055.

Teléfono: 91999999.

Email: rgpd@edipublisa.com

Delegado de protección de datos

Contacto: dpd@edipublisa.com

Finalidad

Le informamos de que el tratamiento de sus datos es necesario para cumplir con nuestras obligaciones del contrato de suscripción, para el envío de nuestro ejemplar semanal y para proceder al giro de los recibos bancarios para el pago de las cuotas mensuales y facilitarle la información que nos solicite. También trataremos la información para mejorar su experiencia de usuario, para ello elaboraremos un perfil comercial con sus preferencias sobre los contenidos de la revista. Su perfil no será utilizado en la toma de decisiones automatizadas.

En el caso de que haya marcado la casilla correspondiente a aceptar ser informado sobre ofertas de productos y servicios de su interés, procederemos al tratamiento de sus datos a tal fin enviándole periódicamente información comercial.

Le informamos de que conservaremos sus datos durante la duración del contrato manteniendo la información el tiempo indispensable para garantizar las obligaciones legales.

Y en el caso de que hubiera manifestado su interés en ser informado sobre nuestra oferta de productos y servicios de su interés, mantendremos su información hasta que nos indique lo contrario.

Legitimación

El tratamiento de datos se efectúa en virtud del contrato de suscripción que usted mantiene con nuestra organización.

Destinatarios

Se informa de que sus datos serán comunicados con el único fin de facilitar el envío de la publicación a entidades de mensajería. También procederemos a la comunicación de sus datos a entidades bancarias para proceder al giro del recibo de suscripción.

No está prevista ninguna comunicación o cesión adicional de información.

Derechos

Le informamos de que puede ejercitar sus derechos, ante nuestro delegado de protección de datos, en la dirección dpd@edipublisa.com o mediante el teléfono 91999999, donde se le facilitará el formulario correspondiente para su solicitud. Se le informa de que deberá acompañar la solución de su DNI como prueba de su identidad.

Podrá ejercer su derecho:

1. Derecho a solicitar el acceso a los datos personales relativos al interesado.

2. Derecho a solicitar su rectificación o supresión.

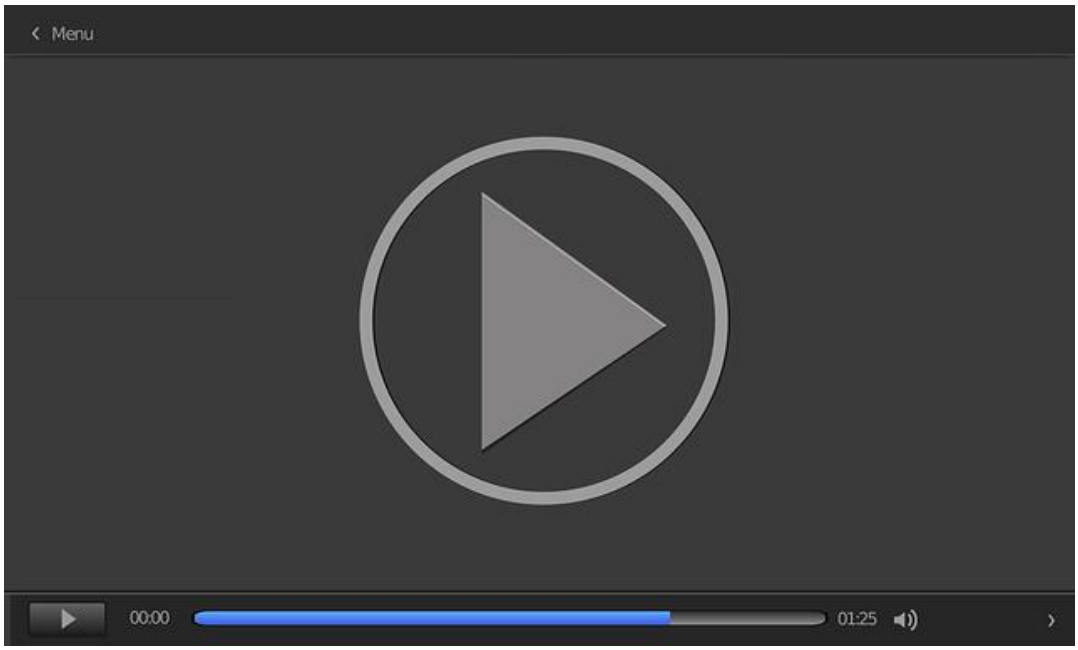
3. Derecho a solicitar la limitación de su tratamiento de sus datos, si bien los conservaremos para el ejercicio o defensa de reclamaciones.

4. Derecho a oponerse al tratamiento como, por ejemplo, a la elaboración de perfiles comerciales.

5. Derecho a la portabilidad de los datos.

Para más información sobre sus derechos, puede consultar con nuestro DPD o en la Agencia Española de Protección de Datos.

Ahora, accede al vídeo *Concienciación en protección de datos.*



Accede al vídeo:

https://unir.cloud.panopto.eu/Panopto/Pages/Embed.aspx?id=8a16658a-a572-4cd2-b98d-b1fb00fe8e7c

8.6. El derecho de interesado

En este aspecto, el RGPD incorpora nuevos derechos que extienden los reconocidos en las legislaciones previas.

Al derecho de información se le unen otros seis derechos.

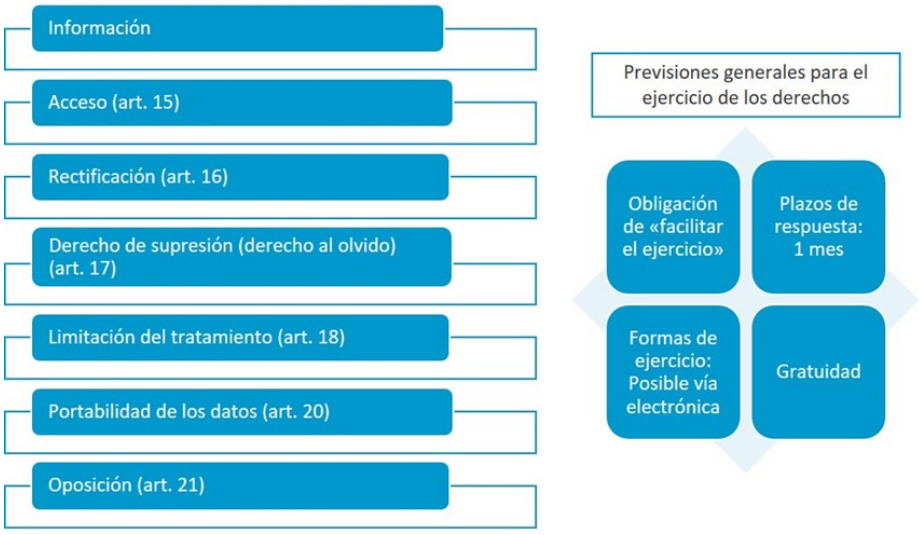


Figura 5. Derechos de interesado. Fuente: elaboración propia.

Derecho de acceso (art. 15, RGPD)

Derecho del titular de los datos (ciudadano) a conocer de la mano del responsable de tratamiento **si se están tratando sus datos o no, y en caso afirmativo tener acceso a sus datos de carácter personal.**

Además, tendrá derecho a:

- Ser informado de las **finalidades del tratamiento** de datos personales.
- El tipo de datos que son recabados (categorías de datos).
- Los **destinatarios de los datos** o categorías de destinatarios a lo que son o serán comunicados los datos.
- Ser informado del derecho a solicitar: la rectificación o supresión de los datos, la limitación del tratamiento, la posibilidad de oponerse al tratamiento.
- Ser **informado del origen de los datos** cuando estos no hayan sido recabados directamente del interesado por parte del responsable de tratamiento.
- La **facultad de poder presentar una reclamación** ante la autoridad de control. Por ejemplo, en España ante la Agencia Española de Protección de Datos.
- **En el caso de decisiones automatizadas, derecho a conocer la lógica y las posibles consecuencias para el afectado** derivadas de esta decisión (art. 22, RGPD).
- En el caso de que los datos sean objeto de **transferencia internacional de datos,** el afectado tendrá **derecho a conocer las garantías que ofrece el país de destino.** (art. 46, RGPD).

El interesado tendrá derecho a acceder a una copia de los datos que son objeto del tratamiento, ahora bien, para copias adicionales el responsable del tratamiento podrá repercutir un coste.

Derecho de rectificación (art. 16, RGPD)

Derecho del titular de los datos (ciudadano) a rectificar los datos inexactos, completar los datos existentes y a que el responsable del tratamiento proceda a la rectificación sin dilación indebida. El retraso puede ser motivo de sanción.

Derecho de supresión (derecho al olvido) (art. 17, RGPD)

Derecho del titular de los datos (ciudadano) a solicitar y obtener, sin retraso no justificado, la eliminación (supresión) de sus datos de carácter personal.

El responsable del tratamiento estará obligado a atender la solicitud de supresión en los siguientes casos:

- Los datos personales ya no son necesarios para los fines que fueron recabados o tratados.
- El interesado retira el consentimiento habilitante del tratamiento (base legal).
- Existe un tratamiento ilícito de los datos personales.
- Por imperativo legal.
- Son datos personales obtenidos en relación con la oferta por parte del responsable del tratamiento de servicios de la sociedad de la información a menores.

En los casos de los datos personales que se hayan hecho públicos, el RGPD introduce una interesante novedad: la obligación del responsable del tratamiento de tomar medidas para informar a aquellos que estén tratando dichos datos personales, sobre la solicitud de supresión de:

- Todo enlace a esos datos personales.
- Cualquier copia o réplica de los datos.

En cualquier caso, la supresión no será aplicable en todas las situaciones, el derecho de supresión está limitado en los casos siguientes:

- El tratamiento es necesario para ejercer el derecho de información o de libertad de expresión.
- Existe obligación legal aplicable que exige el tratamiento.

- En el ámbito de presentación de reclamaciones (formulación, ejercicio o defensa).
- Motivos de interés público en el ámbito de la de salud pública, que es uno de los ámbitos que el art. 9 («Tratamiento de categorías especiales de datos personales») recoge como lícito.
- Con la finalidad de investigación científica o histórica, fines de archivo en interés público o con finalidad estadística.

Derecho a la limitación del tratamiento (art. 18, RGPD)

El derecho a la limitación en el tratamiento de datos que realiza un responsable de tratamiento en determinados casos. Podrá conservar los datos para un uso limitado. Será de aplicación:

- Cuando exista una impugnación por el interesado sobre la exactitud de los datos personales, y será aplicable durante el plazo razonable de verificación de la exactitud por parte del responsable de tratamiento.
- Ante un tratamiento ilícito, que obliga la supresión de los datos, el interesado prefiera que no se suprima, sino que se limite el uso de estos.
- Los datos no son ya necesarios para el responsable del tratamiento, lo que obligaría a la supresión de los mismos, pero sí son datos necesarios por parte del interesado en procesos de reclamaciones.
- Durante el tiempo en el que se evalúa la legitimidad por parte del interesado de oponerse a un tratamiento.

Como norma general para los derechos de rectificación, supresión o limitación del tratamiento, el responsable de tratamiento debe comunicar a los destinatarios de los datos el ejercicio de derechos efectuado (salvo que esto no sea posible o requiera medios desproporcionados).

En cualquier caso, el interesado tendrá derecho a conocer los destinatarios según el artículo 19 («Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento») del RGPD.

Derecho de portabilidad de los datos (art. 20, RGPD)

Derecho a **recibir** por parte del responsable del tratamiento **los datos personales en un formato estructurado, para trasmitirlos a un tercero** o a que los datos se comuniquen directamente a un tercero seleccionado por el usuario. Esto será posible cuando:

- El tratamiento esté basado en el consentimiento del afectado o en un contrato.
- El tratamiento tenga lugar con medios automatizados.

Este derecho faculta la transición de los datos de una forma más eficaz entre los operadores de un sector, motivada por el cambio de cliente de operador, por ejemplo, en telefonía, energía, etc.

Derecho de oposición (art. 21, RGPD)

El derecho a que el interesado pueda oponerse al tratamiento de sus datos personales.

El interesado podrá instar al cese del tratamiento de sus datos personales cuando este tratamiento no esté basado en el consentimiento de afectado y sí en el interés público o el ejercicio de poderes públicos o el interés legítimo del responsable de tratamiento.

En los casos en que el tratamiento de datos tenga una finalidad científica o histórica o estadística, y quede amparado por art. 89 del RGPD, el interesado tiene el derecho a oponerse a que sus datos sean tratados. Derecho que queda limitado si el tratamiento obedece a un interés público.

Un ejemplo de tratamiento basado en un interés legítimo es el **tratamiento de los datos cuya finalidad sea mercadotecnia directa o la elaboración de perfiles.** En este escenario, aunque al responsable le asiste el interés legítimo que le habilitaría para el tratamiento sin el consentimiento del interesado, este tiene el derecho a oponerse al tratamiento de forma total o parcial.

Como expone el RGPD, en el caso de existir un conflicto entre interés legítimo y el derecho del afectado, debe ser el responsable el que «demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado» (considerando 69, RGPD).

Decisiones individuales automatizadas, incluida la elaboración de perfiles (art. 22, RGPD)

El derecho a no ser objeto de decisiones que tengan un efecto jurídico o le puedan afectar significativamente y que se basen en tratamientos automatizados de datos, lo que incluye la elaboración de perfiles, a menos que:

- La decisión sea necesaria para el establecimiento o ejecución de un contrato entre los interesados y el responsable de tratamiento.
- Esté autorizada por la ley.
- Exista un consentimiento explícito del afectado.

En cualquier caso, estas decisiones no pueden basarse en categorías especiales de datos, como «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física» (art. 9.1, RGPD), salvo que sea aplicable alguna excepción de las previstas en el artículo 9.2 como, por ejemplo, el consentimiento explícito del afectado.

En todo caso, será necesario establecer medidas adecuadas para la salvaguarda de los derechos y libertades de los afectados, y también del interés legítimo del interesado.

Limitaciones a los derechos (art. 23, RGPD)

El RGPD reconoce el derecho a que las leyes de la Unión Europea y de los Estados miembros puedan limitar los derechos de los ciudadanos en los casos en los que esto sea necesario para salvaguardar en democracia:

«a) La seguridad del Estado.
b) La defensa.
c) La seguridad pública.
d) La prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.
e) Otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social.
f) La protección de la independencia judicial y de los procedimientos judiciales.
g) La prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas» (art. 23, RGPD).

Las limitaciones a los derechos deberán tener su correspondiente soporte legal. Su aplicación debe seguir preservando el respeto a los derechos y libertades de los ciudadanos, de manera que la limitación al derecho debe estar motivada y debe ser proporcional al fin (bien) que se persigue.

8.7. Obligaciones generales del responsable de tratamiento y encargado

En este epígrafe vamos a aproximarnos a las obligaciones desde la perspectiva de aquellas que deben cumplir las organizaciones que realicen tratamientos de datos de carácter personal, bien por que actúen como **responsable de tratamiento, decidiendo sobre la finalidad** de este, bien como **encargado de tratamiento siguiendo las instrucciones del responsable.**

Es importante que repases las definiciones del apartado Conceptos.

El reglamento tasa las obligaciones de los participantes en el tratamiento y la posible sanción derivada del incumplimiento de estas. De manera que el responsable de tratamiento está obligado a aplicar una serie de medidas que se han identificado como medidas de responsabilidad activa, pensadas para desarrollarse incluso antes de iniciar el tratamiento y durante toda la duración de este, de manera que se garantice que los tratamientos son conformes a la normativa RGPD.

Uno de los aspectos novedosos es el requerimiento de considerar, como base para determinar las medidas técnicas y organizativas destinadas a garantizar el cumplimiento del RGPD, una aproximación basada en el riesgo que el tratamiento específico puede suponer para los derechos y libertades de los afectados por el tratamiento y, lo que es muy relevante, poder demostrarlo (art. 24.1, RGPD).

Por lo tanto, será necesaria la realización de una valoración del riesgo que determinará las medidas más adecuadas para ser aplicadas. Para este análisis habrá que tener en consideración: los tipos de tratamiento efectuados (automatizados, no automatizados), la naturaleza de los datos o categorías de datos para ser tratados, el número de personas afectadas y el número de tratamientos que una organización realice.

En las grandes organizaciones, la AEPD (Agencia Española de Protección de Datos) recomienda que la aproximación a este análisis se efectúe aplicando alguna metodología de riesgos, mientras que, en organizaciones pequeñas, se pueda aproximar con un análisis cualitativo. En este sentido, la AEPD dispone de herramientas para ayudar a la pyme en esta labor. Esta aproximación requiere revisar periódicamente dichas medidas para su evaluación y mejora, y actualizarlas si es preciso (art. 24.2, RGPD), lo que habrá que abordar siempre que la valoración del riesgo del tratamiento pueda verse afectada.

Además, el responsable y encargado de tratamiento deberán llevar registro de las actividades de tratamiento de datos personales que realizan, debiendo estar identificados y documentados.

Uno de los objetivos clave del RGPD es garantizar la protección de los datos desde el diseño (art. 25.1, RGPD), aplicar medidas técnicas y organizativas para dar cumplimento al RGPD, ya desde el momento de elección de los medios de tratamiento para darles continuidad durante toda la duración de este. Un ejemplo, la pseudonimización:

> «La aplicación de la pseudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos» (considerando 28, RGPD).

Ideas clave

La introducción de la pseudonimización como medida no excluye la aplicación de otras medidas destinadas a reducir los riesgos del tratamiento, pero sí se pretende generalizar su uso como medida de no difícil implementación y que facilita la mitigación del riesgo en mayor o menor medida en función del tratamiento de datos personales, los mecanismos de reversibilidad existentes y la seguridad de estos.

El RGPD incorpora, así mismo, la protección de datos por defecto (art. 25.2, RGPD), la aplicación de medidas técnicas y organizativas que garanticen por defecto que solo sean tratados los datos mínimos estrictamente necesarios para la finalidad del tratamiento. Esto obliga a la minimización de datos personales recogidos, la extensión de su tratamiento, la minimización del plazo de su conservación y de su accesibilidad.

El artículo 25 del RGPD recoge la posibilidad de que el responsable de tratamiento pueda utilizar como elemento de prueba del cumplimiento de sus obligaciones el modelo de certificación que recoge el RGPD en su artículo 42, que veremos más adelante.

Por ejemplo, en el caso de una red social donde los datos personales no se pongan a disposición de un número amplio de personas, a menos que el afectado así lo establezca. Es decir, que el usuario pueda, por un lado, decidir la información a la que tendrá acceso la comunidad de la red social con sus diferentes segmentos y que, por otro, al crear un perfil este se configure por defecto sin acceso público.

Por otra parte, los roles de los participantes en el tratamiento específico deben estar claros y definidos, por ejemplo, cuando un tratamiento cuenta con más de un responsable debido a que hay más de una organización y conjuntamente determinan los objetivos del tratamiento y sus medios. En estos casos, el RGPD requiere que el reparto de responsabilidades sea acordado entre las partes formalmente, en lo referente a las obligaciones del RGPD y el derecho a información, teniendo los afectados derecho a acceder a los aspectos esenciales del acuerdo. (art. 26, RGPD).

En estos casos los interesados tendrán derecho a acudir a cualquiera de los corresponsables de tratamiento.

Además, las prestaciones de encargados a responsables de tratamiento serán contractualmente establecidas de conformidad a los requerimientos de la norma. Es decir, habrá contrato formal y especificación de responsabilidades.

A continuación, se presenta un cuadro resumen, de **las medidas de responsabilidad activa** a las que está obligado a aplicar el responsable de tratamiento (art. 27, RGPD).

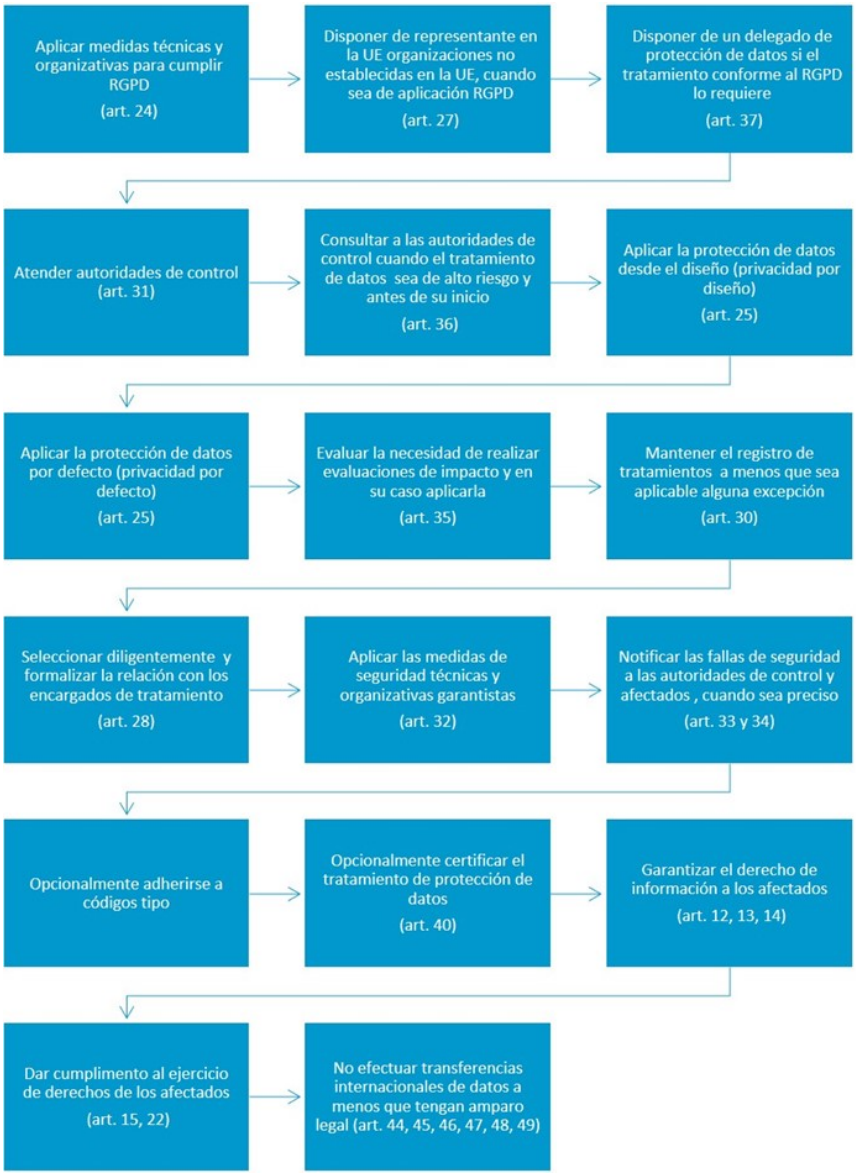


Figura 6. Medidas de responsabilidad activa. Fuente: elaboración propia.

Responsabilidad del encargado de tratamiento

El RGPD transfiere al responsable de tratamiento (RT) l a **obligación de actuar diligentemente** en los casos en que necesite para llevar a cabo el tratamiento de datos personales a un tercero, a un encargado de tratamiento (ET). De hecho, el responsable del tratamiento tiene la responsabilidad de que el encargado de tratamiento disponga y aplique las medidas técnicas y organizativas requeridas por el RGPD. Aunque el tratamiento se encargue a un tercero (encargado de tratamiento), **el responsable de tratamiento debe velar por el cumplimiento del RGPD.** Además, **deberá existir entre las partes un contrato o equivalente** que fije:

- El objeto del tratamiento.
- La duración.
- La finalidad y naturaleza de este.
- El tipo y categorías de datos personales.
- Las categorías de interesados.
- Las obligaciones del responsable de tratamiento.
- Las obligaciones del encargado de tratamiento, como mínimo:
  - Obligación de tratar los datos únicamente siguiendo instrucciones del RT.
  - La obligación de confidencialidad del personal participante en el tratamiento
  - La aplicación de las medidas seguridad (art. 32, RGPD).
  - Autorización para subcontratación, y esta incorpora las mismas obligaciones ya establecidas entre RT y ET (principal).
  - La supresión o devolución de datos al finalizar el tiramiento a elección del RT.

- Facilitar al RT su capacidad de control y supervisión del cumplimiento de sus obligaciones —por ejemplo, mediante auditorías– y de prueba de cumplimiento por parte del ET de sus obligaciones.

Para facilitar la relación entre RT y ET, el RGPD recoge la posibilidad de que la relación se fundamente con base en cláusulas tipo a establecer por las autoridades de control.

Además, se activan mecanismos de certificación en el cumplimiento del RGPD y la adhesión a códigos de conducta como elementos probatorios de la capacidad de ofrecer garantías suficientes para el cumplimiento de las obligaciones establecidas en el RGPD (arts. 42 y 43, RGPD).

Si un ET infringe el RGPD, al determinar los medios y fines de tratamiento (que es obligación del RT), será considerado a todos los efectos RT y, por consiguiente, le serán exigidas las responsabilidades correspondientes como, por ejemplo, la prueba de disponer del consentimiento de los afectados para el tratamiento de datos personales.

Registro de actividades de tratamiento (RAT) (art. 30, RGPD)

El RGPD determina la obligación de que el RT o representante legal lleven a cabo el registro documentado de las actividades de tratamiento de datos que se realizan. Es decir, **las actividades de tratamiento deben estar documentadas.** Este registro debe incluir:

- Nombre, datos de contacto del RT y si aplica corresponsable de datos, representante o delegado de protección de datos (DPO).
- La finalidad o finalidades del tratamiento de datos.
- Descripción de las categorías de interesados: clientes, trabajadores, alumnos, etc.

Ideas clave

- Descripción de las categorías de datos personales tratados: identificación, salud, financieros, etc.
- Categorías de destinatarios a los que se comunicarán los datos: sector de actividad o grupos de actividad a los que pertenecen.
- En caso de que existan transferencias internacionales de datos, documentación de las garantías que presenta el tratamiento para las libertades y protección de datos que ampara la transferencia en el marco del RGPD incorporando la descripción del principio aplicado para la legitimación de las transferencias internacionales, así como la justificación de la aplicación de excepciones del artículo 49 del RGPD (que veremos más adelante).
- Plazos previstos para la supresión de los datos personales (de las categorías de datos): máximo tiempo que se mantendrán los datos o criterios para su cancelación.
- Descripción general de medidas técnicas y organizativas de seguridad aplicadas (art. 32.1, RGPD).

Además, la obligación de mantenimiento de un registro se extiende también al encargado de tratamiento:

- Nombre, datos de contacto del encargado de tratamiento, del responsable del tratamiento por cuenta del cual se efectúa el tratamiento de datos (quién contrata), representantes y delegado de protección de datos (DPO) y si aplica categorías de tratamientos realizados por cuenta del RT.
- En caso de que existan transferencias internacionales de datos, incluirá la documentación de garantías para las libertades y protección de datos que ampara la transferencia internacional en el marco del RGPD. En situaciones en las que el encargado de tratamiento realiza la exportación internacional de los datos para que estos sean tratados por una filial del grupo, se debe justificar el amparo legal a la misma.

- Descripción general de medidas técnicas y organizativas de seguridad aplicadas conforme al artículo 32.1 del RGPD.

Si la empresa u organización emplea a **menos de 250 trabajadores** no se le aplicarán la obligación de registro, siempre y cuando:

- El tratamiento de datos por realizar no entraña riesgo para los derechos y libertades de los ciudadanos.
- Es ocasional.
- No incluye categorías de datos especialmente protegidas o datos relativos a condenas e infracciones penales (art. 10, RGPD).
- Esto facilitara el tratamiento de datos a pequeñas empresas de sectores como los servicios no sociosanitarios.
- La notificación previa de los tratamientos a las autoridades de control en materia de protección de datos se había desarrollado de manera desigual en los países miembros de la UE, tanto en alcance de los tratamientos de obligada notificación, así como en el coste administrativo para los responsables de tratamiento. Con la entrada en vigor del RGPD, esta previsión desaparece. Por tanto, la necesidad de llevar este registro implicará la desaparición de la preceptiva inscripción de ficheros, previa al inicio del tratamiento (como era el caso de España ante la Agencia Española de Protección de Datos).

Cooperación con las autoridades de control (art. 31, RGPD)

Los ET y RT están obligados a colaborar directamente o a través de sus representantes con las agencias de protección de datos.

Obligaciones sobre la seguridad de los datos

El RGPD también incorpora la seguridad como principio de protección de datos, como ya veíamos en el artículo 5, donde se especifica este principio sobre el tratamiento de datos de carácter personal, que deberán ser «tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad)» (art. 5.1.f, RGPD).

La aplicación de este principio necesariamente se traduce en **obligaciones para el responsable de tratamiento y para el encargado de tratamiento,** como se establece en el artículo 32 («Seguridad del tratamiento»), donde se **requiere** a ambos la **aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado.** Para ello se tendrán en cuenta:

- El estado de la tecnología.
- Los costes de aplicación.
- La naturaleza del tratamiento y de los datos objeto de tratamiento.
- El alcance (el número de afectados, la duración…).
- El contexto.
- Los fines del tratamiento.
- Los riesgos, probabilidad y gravedad, variables para los derechos y libertades de las personas físicas.

Estableciendo que al menos deberán aplicarse las siguientes medidas técnicas y organizativas (art. 32, RGPD):

- La **pseudonimización** de los datos personales, ya comentada anteriormente.
- El **cifrado** de datos personales.
- **Medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia** (la capacidad de un sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido tanto de los sistemas como de los servicios de tratamiento).
- **Medidas para restaurar la disponibilidad de los sistemas y servicios de tratamiento** y el acceso a los datos de carácter personal, de un modo rápido en los casos de incidentes físicos (incendio, avería, etc.) o técnicos (corrupción de sistemas, etc.).
- Aplicar un proceso regular para la **verificación, evaluación y valoración de las medidas** tanto técnicas como organizativas para garantizar la seguridad del tratamiento.

Es importante resaltar que deberán tomar medidas para que cualquier individuo que participe en el tratamiento de datos personales solo pueda tratar dichos datos a partir de las instrucciones del responsable de tratamiento (art. 32.4, RGPD).

Un aspecto de potencial dificultad es la evaluación de la adecuación del nivel de seguridad aplicado teniendo en cuenta los riesgos que presenta el tratamiento para los derechos y libertades de los afectados. Para ello el artículo 32 introduce como criterio de evaluación «los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (art. 32.2, RGPD). En cualquier caso, no será fácil.

Para facilitar esta aproximación, el tercer punto del artículo 32 facilita la adhesión por parte del responsable de tratamiento a un **código de conducta** que haya sido aprobado por las autoridades de control (art. 40, RGPD) o la posibilidad de someter su sistema a un proceso de certificación, como prueba de cumplimiento de los requerimientos en materia de seguridad y del resto de sus obligaciones por parte del responsable de tratamiento de sus obligaciones en el marco del RGPD.

De manera que tanto el cumplimiento de códigos de conducta y la certificación opcional serán mecanismos que permitan mostrar por parte del responsable de tratamiento o encargado de tratamiento el cumplimiento de sus obligaciones.

Ante un incidente o evento de seguridad, no le eximirán de potenciales responsabilidades, pero si serán prueba de descargo ante un procedimiento sancionador.

Por consiguiente, los aspectos que veremos posteriormente tanto de certificación como de establecimiento de códigos de conducta adquieren un central protagonismo por la capacidad que estos deben aportar para objetivar los criterios de evaluación de la adecuación de las medidas técnicas y organizativas.

Notificaciones de violaciones de seguridad de los datos personales a la autoridad de control

El reglamento establece como medida de seguridad adicional y de transparencia la obligación para los responsables de tratamiento **de notificar a la autoridad de control que le corresponda la violación de seguridad en un plazo de 72 horas.** En el caso de que no se efectúe esta notificación en el plazo establecido por un retraso, deberá argumentarse los motivos del retraso (hay que recordar que la autoridad de control se determina en virtud de la aplicación del artículo 55). La notificación deberá incluir la siguiente información:

- Una descripción de la violación de seguridad y, si es posible, las categorías de datos afectados, así como dimensionar el número de interesados afectados y de registros de datos de carácter personal.
- Datos de contacto para ampliar información. Generalmente, serán los datos del delegado de protección de datos.
- Describir los riesgos o consecuencias de la violación sufrida.
- Declarar las medidas técnicas y organizativas adoptadas o propuestas para finalizar con la violación y, si procede, para reducir los riesgos para los afectados.

Como no siempre será posible disponer de toda la información indicada de un modo inmediato y en el plazo establecido, el reglamento permite que se pueda facilitar dicha información de manera progresiva (art. 33.4, RGPD).

Hay que recordar que la no notificación de la violación puede ser objeto de sanción.

Como obligación general, el RT deberá llevar un registro de violaciones incorporando todos los elementos relevantes relacionados con la violación, los efectos ocasionados y las medidas correctoras aplicadas. Este registro quedará a disposición de la autoridad de control.

Comunicación de violaciones de seguridad a los interesados

Como medida adicional de transparencia, según el artículo 34 del RGPD, cuando exista un alto riesgo para los derechos y libertades de los ciudadanos, el responsable de tratamiento estará obligado a comunicar la situación a los afectados, informando de las características de la violación de seguridad y de las medidas adoptadas.

Esta comunicación no será necesaria siempre que se den alguna de las siguientes condiciones:

- La violación afecte a datos cifrados, por lo que el riesgo de acceso a datos personales sea despreciable.
- Que se tomaran medidas inmediatamente después de la violación que permitan considerar que no existe alta probabilidad de que potenciales perjuicios se materialicen para los afectados.
- Que suponga un esfuerzo ímprobo, en cuyo caso bastará con una notificación pública.

Ideas clave

Evaluaciones de impacto

En los casos en los que es probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable de tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (PIA: *privacy impact assessment*) (art. 35, RGPD). ¿Cuándo habrá que realizar un PIA, atendiendo al RGPD? Cuando estemos en los siguientes escenarios:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado.
- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente.
- Tratamiento a gran escala de categorías especiales de datos o datos penales.
- Observación sistemática a gran escala de una zona de acceso público. Videovigilancia.

El RGPD establece el marco general de aplicación del PIA, pero reconoce a las autoridades de control la capacidad de determinar qué tratamientos (arts. 35.4 y 35.5, RGPD), por su naturaleza, deberán ser sometidos a un PIA. Por lo que progresivamente se irán concretando tratamientos en los que será requerido y aquellos en los que se considere de no aplicación.

A modo de resumen, hay que indicar que una evaluación de impacto, en línea con el RGPD, deberá incluir como mínimo:

- Descripción de los tratamientos de datos previstos, de sus finalidades y, si el tratamiento se sustenta en un interés legítimo, la especificación de este.
- Una evaluación de la necesidad del tratamiento propuesto y la proporcionalidad de dicho tratamiento con respecto las finalidades perseguidas.

- Una evaluación de los riesgos que el tratamiento pueda implicar para los interesados en lo referente a sus derechos y libertades.

- Las medidas que serán de aplicación para mitigar los riesgos mencionados, medidas para garantizar la seguridad y justificación de conformidad del tratamiento con el RGPD.

Siempre que exista un cambio en el perfil de riesgo del tratamiento, será preciso efectuar una revisión del PIA.

Si el resultado del PIA identificara que el tratamiento de datos personales es de alto riesgo, el responsable de tratamiento deberá consultar ante la autoridad del control, que se pronunciará por escrito para asistir al responsable para incorporar medidas adicionales requeridas y dar viabilidad al tratamiento (art. 36, RGPD).

Delegado de protección de datos

El RGPD establece la obligación de nombrar un delegado de protección de datos (DPD). Esta es una figura nueva en el ordenamiento jurídico, aunque converge con las tendencias corporativas de identificación del *data privacy officer.*

Las funciones que ha de desempeñar el DPD incluyen:

- **Informar o asesorar** al responsable de tratamiento (en su caso, al encargado de tratamiento) y a sus empleados de las obligaciones que establece el Reglamento General de Protección de Datos.

- **Supervisar** que se da un adecuado **cumplimiento de la normativa** en los tratamientos de datos realizados por la organización y de sus políticas internas en materia de protección de datos personales, supervisando las asignaciones de responsabilidades, la concienciación y formación del personal y de las auditorías.

- Ser responsable de **supervisar la aplicación de evaluaciones de impacto** y asesorar al respecto, en los casos en que la organización esté obligada.

Ideas clave

- Ser el **punto de contacto con las autoridades de control** y cooperar con ellas.
- Los datos de contacto del delegado de protección de datos deben ser públicos y, además, ser notificados a la autoridad de control correspondiente.
- Estar **a disposición de los interesados para los procesos de ejercicio de derechos por parte de los interesados.**
- Actuar **con independencia y reportando a la dirección** de la organización.

El perfil de un delegado de protección de datos (DPD) o *data protection officer* (DPO) necesita amplios conocimientos en derecho y en la práctica de la protección de datos personales, pero el reglamento no determina exactamente qué titulación debe ostentar el profesional para su desempeño como DPD.

Para dar respuesta a esta cuestión y con objeto de incorporar elementos tangibles y de confianza en el ejercicio profesional, desde la Agencia Española de Protección de Datos **se ha desarrollado el marco para la certificación del DPD,** una iniciativa pionera que desarrolla junto con la Entidad Nacional de Acreditación (ENAC) conforme a la norma UNE-EN ISO/IEC 17024:2012. La certificación está llamada a ser garante de las capacidades del DPD con relación a sus conocimientos y experiencia frente a los responsables de tratamiento, es decir, es una certificación profesional individual.

Las entidades certificadoras serán las acreditadas por parte de la ENAC y la certificación es voluntaria. Es decir, no hay obligación por parte del DPO de estar certificado.

Se puede acceder al esquema de certificación desde la web de la AEPD:
https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

El nombramiento del DPO, que puede ser personal interno o externo, **será obligatorio** siempre que:

- El **tratamiento lo lleve a cabo una autoridad u organismo público** (excepto los tribunales que actúen en ejercicio de su función judicial).
- Las actividades principales del responsable o del encargado de tratamiento consistan en **operaciones de tratamiento que**, debido a su naturaleza, alcance o fines, **requieran una observación habitual y sistemática de interesados a gran escala**, como los casos de videovigilancia o seguimiento de actividad en Internet.
- Las actividades principales del responsable o del encargado consistan en el **tratamiento a gran escala de categorías especiales de datos personales,** como son los datos de salud.

Debemos resaltar que los **grupos empresariales podrán disponer de un único DPD.**

Responsabilidades civiles y penales de los responsables o encargados de tratamiento

El incumplimiento de sus obligaciones por parte de responsables y encargados de tratamiento puede implicar responsabilidades de diversa índole:

- **Responsabilidad penal:** depende del código penal de cada uno de los países miembros de la UE, no existiendo una homogeneización en este sentido para el supuesto penal. A modo de ejemplo en la legislación española, el artículo 197 del Código Penal (capítulo I: «Del descubrimiento y revelación de secretos»):

SUPUESTOS	PENAS
Aquellos que descubran secretos o vulneren la intimidad de los interesados sin el consentimiento de estos, accediendo al correo o interceptando comunicaciones, realizando escuchas.	De 1 a 4 años, multas de 12 a 24 meses.
Aquellos que se apoderen, modifiquen o utilicen datos de carácter personal en perjuicio de un tercero (por ejemplo, la revelación o divulgación de imágenes personales).	De 1 a 4 años, multas de 12 a 24 meses.
Aquellos que, sin haber participado directamente en la obtención de la información personal «robada», sí participan en su divulgación.	Entre 2 y 4 años.
Las actividades ilícitas mencionadas son llevadas a cabo por el responsable de tratamiento.	De 3 a 5 años.
Si existe ánimo de lucro.	Hasta 7 años.
Aquellos que divulguen a terceros imágenes o grabaciones captadas inicialmente con el consentimiento del afectado y que atenten gravemente a la intimidad personal de esa persona.	- De 3 meses a 1 año o multa de 6 a 12 meses. - De 2 a 6 años o multa de 12 a 24 meses en caso de que exista relación afectiva, la víctima sea menor de edad o exista fin lucrativo.

Tabla 2. Supuestos y penas. Fuente: art. 197, Ley Orgánica 10/1995, de 23 de noviembre.

- **Responsabilidad administrativa:** deriva en sanciones administrativas impuestas por la autoridad competente. Como es el caso de las sanciones de las autoridades de control de protección de datos (en España, la Agencia Española de Protección de Datos).

- **Responsabilidad civil:** puede suponer el pago de indemnizaciones por los perjuicios sobre los afectados derivados del incumplimiento de la normativa en protección de datos.

8.8. Otros marcos internacionales

Son numerosas las iniciativas establecidas en formalizar marcos de referencia para garantizar la privacidad en los tratamientos de datos de carácter personal y que no tienen un componente legal. Entre las más interesantes tenemos:

- Principios Generales de la Protección de Datos de ODCE.
- ISO/IEC 29100:2011. Information technology. Security techniques. Privacy framework.
- ISO/IEC 27701:2019. Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guideline.

Entre ellos no es difícil encontrar amplias similitudes respecto a los principios que establecen para el tratamiento de datos personales, si bien los desarrollos de estos marcan las diferencias.

Así, no es difícil establecer un **mapeo** entre los diferentes marcos de protección de la privacidad, mostrando su convergencia.

Principios de privacidad OCDE	Principios de privacidad ISO/IEC
1. Limitación a la recolección	1. Consentimiento y elección 3. Limitación a la recolección
2. Calidad de datos	6. Exactitud y calidad
3. Especificación del propósito	2. Legitimidad de propósito y especificación
4. Limitación en el uso	4. Minimización de datos 5. Limitación de uso, retención y divulgación:
5. Seguridad y salvaguardas	10. Seguridad de la información
6. Apertura	7. Apertura, transparencia y notificación
7. Participación individual	8. Participación individual y acceso
8. Responsabilidad *(accountability)*	9. Rendición de cuentas 11. Cumplimiento de la privacidad

Tabla 3. Mapeo de marco de privacidad. Fuente: Brandon y de Souza, 2016.

ISO/IEC 27701:2019, extensión de privacidad de la ISO/IEC 27001:2013

En 2019, se publica la ISO/IEC 27701:2019 (Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guideline) con el objetivo de mejorar el sistema de gestión de seguridad de la información (SGSI) vinculado a la ISO/IEC 27001:2013, con requisitos adicionales para establecer, implementar, mantener y mejorar un sistema de gestión de información de privacidad (PIMS). La ISO/IEC 27701:2019 Es una norma certificable.

8.9. Protección de datos en EE. UU. y otros países

La regulación en materia de protección de datos personales es muy dispar a nivel internacional, existiendo notables diferencias entre los marcos regulatorios, tanto desde el punto de vista del ámbito de aplicación como de los derechos reconocidos.

Analizando la legislación de diferentes estados se identifican dos aproximaciones legislativas muy diferentes atendiendo a su tradición jurídica:

- Estados con un marco regulatorio general y completo, con leyes de tipo ómnibus que en algunos casos se complementan con regulaciones sectoriales.
- Estados que cuentan con múltiples normas jurídicas sectoriales o territoriales, por lo que en muchos casos resulta complejo identificar todas y cada una de las normas aplicables.

También se encuentra una amplia disparidad en lo referente a los derechos y obligaciones que establece la ley y el amparo que las mismas dan a los ciudadanos en relación con el tratamiento de sus datos personales.

En la siguiente infografía se recoge esta visión por parte de un relevante bufete internacional en el ámbito de la protección de datos, DLA Piper.

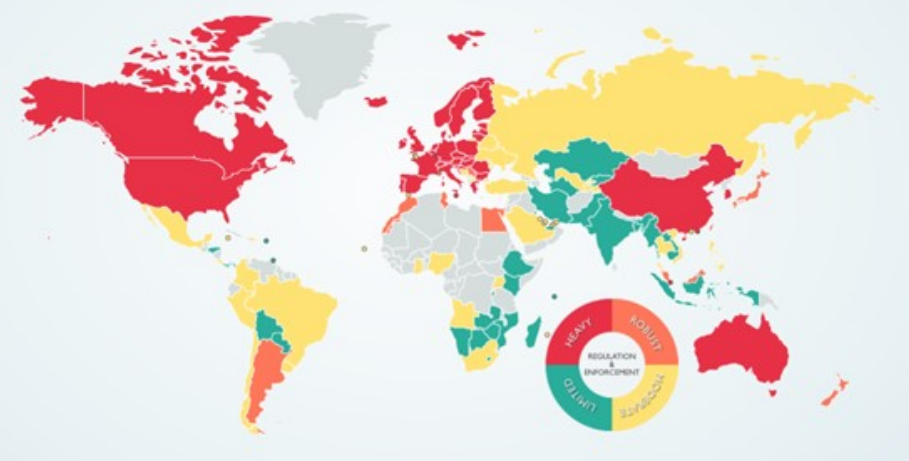


Figura 7. Protección de datos alrededor del mundo. Fuente: Avram et al., 2020.

Puedes acceder a la información de DLA Pipper sobre la situación legislativa internacional en la web:
https://www.dlapiperdataprotection.com/

En Iberoamérica, cabe resaltar la situación de Argentina, que desde el 30 de junio de 2003 tiene el reconocimiento de la Comisión Europea de ofrecer un nivel adecuado de protección de datos personales.

Protección de datos en EE. UU.

Son muchos los que encuentran en EE. UU. los antecedentes de la privacidad y la protección de datos personales y el carácter inspirador de esta para la normativa europea en sus orígenes.

En 1798, la cuarta enmienda de la Constitución de EE. UU. reconoció el derecho de los ciudadanos a la inviolabilidad del domicilio, pero no sería hasta el siglo XIX cuando el concepto de privacidad moderno tomaría cuerpo en la sociedad estadounidense, a partir del debate social emergente que cuestionaba el amparo sobre la vida privada que ofrecía la ley.

Ideas clave

De hecho, a finales del siglo, los juristas norteamericanos Samuel Warren y Louis Brandeis, los que lideran el concepto jurídico de **derecho a la vida privada** *(privacy law),* en un artículo publicado en la revista de la Universidad de Harvard con el título «The right to privacy» introdujeron por primera vez la privacidad como acción civil y promovieron la creación de un nuevo derecho civil de amparo al espacio personal frente a su difusión al público no autorizada.

Pero deberían pasar años hasta la consolidación del derecho a la privacidad, que en EE. UU. integra cuatro ámbitos: la esfera privada, la apropiación del nombre, la distorsión de la imagen y la difusión pública de hechos privados; para que a través de un conjunto de normas se fuera consolidando dicho derecho:

- *Privacy Act* (Ley de protección a la Intimidad de 1974).
- *Freedom of Information Act* (Ley de Libertad de la Información, FOIA).
- *Fair Credit Reporting Act* (Ley de Equidad Financiera de 1978).
- *Privacy Act* (Ley de protección de la Intimidad de 1974).

La Ley de Protección a la Intimidad de 1974 tiene por objeto la protección de la intimidad de las personas, cuyos datos personales figuran en bancos de datos del gobierno, incorporando los siguientes principios:

- La prohibición de la existencia de bancos de datos personales secretos.
- El derecho del ciudadano a conocer la información tratada y la finalidad de dicho tratamiento.
- El derecho a corregir la información registrada.
- La prohibición del tratamiento de datos personales para otras finalidades para las que fueron recabados sin consentimiento del titular.

Ideas clave

La *Privacy Act,* que sería posteriormente modificada entre otros por las enmiendas surgidas de las leyes de Libertad de la Información *(Freedom of Information Act),* es de aplicación a las bases de datos del Gobierno federal con ciertas limitaciones, como son los archivos de los servicios de inteligencia, inmigraciones, lucha con el narcotráfico, etc., y reconoce el derecho de acceso a la información personal.

En este punto podemos encontrar cierta similitud con los principios que rigen la protección de datos en la UE. Pero, como indicaba, es una ley que afecta solo al Gobierno federal y es que el sistema jurídico anglosajón se desarrolla en torno a leyes sectoriales en lugar del establecer un marco general regulador, tipo ómnibus, como es el caso de la UE y de España.

Por ello no es difícil encontrar un conglomerado de normas a nivel federal o incluso estatal que versan sobre el derecho a la privacidad. EE. UU. dispone del entorno de 20 normas específicas o que abordan ampliamente la privacidad o la seguridad de los datos personales como, por ejemplo, *Fair Credit Reporting Act* de 1978, que regula aspectos del tratamiento de datos de los individuos por parte de las entidades financieras, exigiendo ciertas garantías de confidencialidad sobre el acceso por parte del Gobierno y por las agencias de información de crédito.

A ello se suman cientos de desarrollos normativos específicos de los Estados miembros. Por ejemplo, California dispone de más de 25 normas sobre privacidad y seguridad de datos.

En general, la normativa exige que sea preceptiva la información previa a la recolección de los datos, especialmente cuando se trata de datos considerados sensibles (la que versa sobre la salud, información financiera, la correspondiente a menores de 13 años…) y la utilización de los datos para finalidades permitidas.

En relación con la existencia de requerimientos de seguridad, las leyes tanto en el ámbito estatal como federal incorporan obligaciones destinadas a garantizar la confidencialidad de la información y no son pocos los Estados en los que es obligatorio comunicar la existencia de brechas de seguridad que hayan supuesto el acceso a datos de personales.

En EE. UU. no existe un organismo de control general en materia de protección de datos, como sí ocurre en los Estados miembros de la UE, pero sí dispone de instituciones o autoridades de vigilancia y control sectoriales como, por ejemplo, la Federal Trade Comission (FTC), entidad con la que se desarrolla los principios de *privacy shield*.

Protección de datos en EE. UU. y la UE

Aunque existen amplios puntos de convergencia entre las normativas de EE. UU. y la UE, las primeras ideas sobre protección de datos a ambos lados del Atlántico nacen en la década de los 70 y uno de los fundamentos de los principios recogidos en el Convenio de Protección de Datos del Consejo de Europa (1981) tenía como inspiración los principios de información justa (*Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens,* 1973), principios que también inspiraron las directrices de privacidad de la OCDE (1980).

Sin embargo, estos principios evolucionaron de forma diferente: en EE. UU. apostaron por la autorregulación, mientras que en la UE llegaron a la consideración de derecho fundamental, vinculante en el Tratado de Lisboa de 2009.

Por ello, el modo y alcance en el que se reconocen los derechos en torno a la protección de datos presentan notables divergencias:

- En la propia concepción del derecho que ya se manifiesta en la cuarta enmienda de la Constitución de EE. UU., con un alcance más limitado que el derecho a la vida privada que reconoce el artículo 7 de la Carta de la UE, donde «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones» (art. 7, Carta de los Derechos Fundamentales de la Unión Europea).

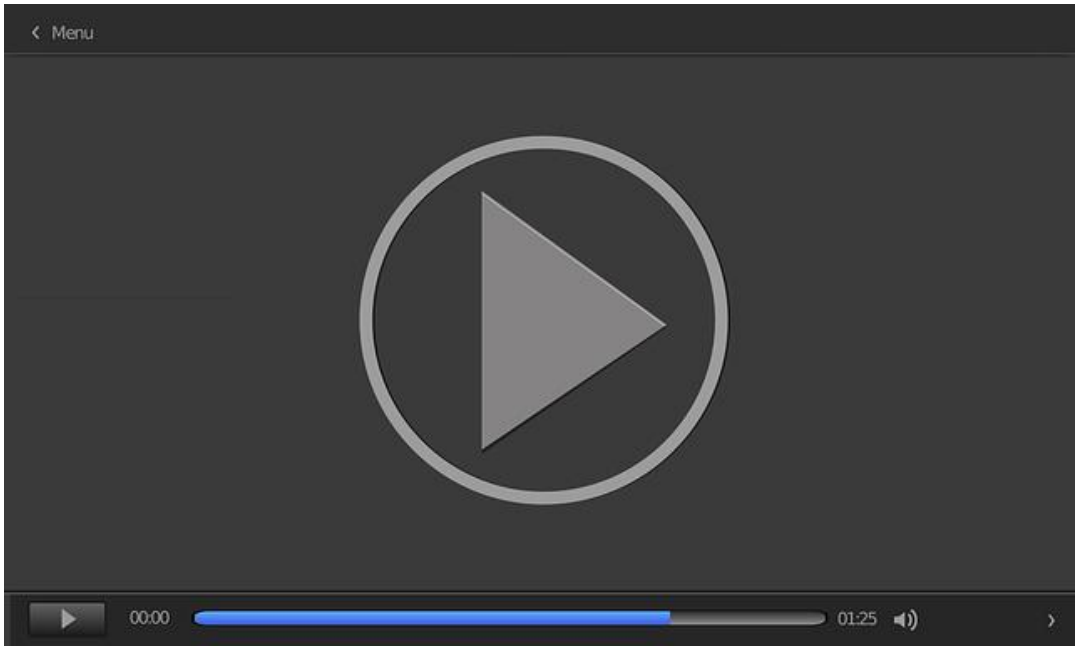
- En la sustancial diferencia en la concepción de datos personales. En la UE, como hemos visto, abarca toda información que identifica o hace identificable a una persona. Una definición mucho más amplia que la extendida en EE. UU., que se centra más en el dato que identifica y no en el dato que hace posible la identificación de las personas. También es posible encontrar alguna excepción a esto. Por ejemplo, en la nueva regulación COPPA *(Children´s online privacy protection rule)* del FTC se reconoce como dato personal el identificador persistente que pueda ser utilizado para reconocer a un usuario en el tiempo a lo largo de diferentes webs o servicios *online*.

Esta concepción hace que la ley de EE. UU. se centre en reparar el daño al consumidor y la búsqueda de un adecuado equilibrio entre privacidad y las necesidades relacionadas con las transacciones comerciales que fundamenta la no existencia de restricciones en EE. UU. en relación con la exportación de datos (excepto para ciertas informaciones gubernamentales), con un impacto significativo en los flujos de datos internacionales. Un escenario en el que las organizaciones y las empresas de la UE se ven sometidas a muchas más restricciones que las de EE. UU.

Las implicaciones de estas divergencias y su impacto están detrás del debate dentro de la comunidad en busca de una mitigación de las barreras existentes a través de una aproximación en el concepto de dato personal en EE. UU. Por ejemplo, de PII

2.0. *(personal identification information),* que incorporaría al concepto de dato personal en EE. UU. los datos de personas identificables y la evaluación continua del riesgo de identificación.

Para terminar con este apartado, accede al vídeo *Las evaluaciones de impacto.*



Accede al vídeo:

https://unir.cloud.panopto.eu/Panopto/Pages/Embed.aspx?id=d9969afc-8ea5-4671-9259-b1fb00fe8e5b

8.10. Transferencias internacionales de datos

Una de las motivaciones principales de establecer un marco común de protección de los datos de carácter personal es la de facilitar el movimiento transfronterizo de datos. En esta línea no solo tenemos el Reglamento General de Protección de Datos, sino también otras iniciativas como las de la OCDE *(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).*

En este sentido, el RGPD sigue los mismos principios consolidados en la UE, que garantiza que el **movimiento de datos entre países miembros de la UE no está limitado.** Pero también se van a permitir aquellos movimientos internacionales de datos fuera de la UE, siempre que se cumplan con los requerimientos establecidos.

Figura 8. Transferencia de datos personales. Fuente: elaboración propia.

- **Transferencias basadas en una decisión de adecuación de la Comisión** (art. 45, RGPD): identifica a los países que tienen un marco de protección de datos de garantías equivalentes al de la UE. Para ello, la Comisión, según el RGPD, tendrá en consideración: el estado de derecho en relación con los derechos humanos y las libertades fundamentales, la existencia de mecanismos de control mediante autoridades independientes y los compromisos internacionales.

En la actualidad, la lista de países que ostenta esta consideración y a los que se puede realizar una exportación de datos legal bajo este principio son países con un nivel adecuado de protección, declarados hasta la fecha son los siguientes:

- **Suiza.** Decisión 2000/518/CE de la Comisión, en 2000.
- **Andorra.** Decisión 2010/625/UE de la Comisión, en 2010.
- **Canadá.** Decisión 2002/2/CE de la Comisión, en 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, en 2003.
- **Uruguay.** Decisión 2012/484/UE de la Comisión, en 2012.
- **Guernsey.** Decisión 2003/821/CE de la Comisión, en 2003.
- **Isla de Man.** Decisión 2004/411/CE de la Comisión, en 2004.
- **Jersey.** Decisión 2008/393/CE de la Comisión, en 2008.
- **Islas Feroe.** Decisión 2010/146/UE de la Comisión, en 2010.
- **Israel.** Decisión 2011/61/UE de la Comisión, en 2011.
- **Nueva Zelanda.** Decisión 2013/65/UE de la Comisión, en 2012.
- **Japón.** En 2019.

Ideas clave

- **Transferencias internacionales mediante garantías adecuadas** (art. 46, RGPD): cuando no existe una decisión por parte de la Comisión de adecuación, se puede recurrir a otros mecanismos que ofrecen garantías adecuadas, reconocidos por el RGPD:

  - Instrumentos que vinculen jurídicamente y exigibles entre autoridades u organismos públicos.
  - Normas corporativas vinculantes (art. 47, RGPD).
  - Las cláusulas tipo de protección de datos, adoptadas por la Comisión.
  - Las cláusulas tipo de protección de datos personales, adoptadas por una autoridad de control y que hayan sido aprobadas por la Comisión.
  - Con base en el código de conducta junto a compromisos vinculantes y exigibles en el país destinatario.
  - Con base en la certificación junto a compromisos vinculantes y exigibles en el país destinatario.
  - Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional que hayan sido autorizadas por la autoridad de control competente.
  - Disposiciones incluidas en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados y sobre los que se haya pronunciado positivamente la autoridad de control.

- Fuera de estos casos, la legitimación de una transferencia internacional debe estar sustentada por alguna de las siguientes **excepciones** (art. 49, RGPD):
  - **Consentimiento explícito** del interesado a la transferencia de datos, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas.
  - **Necesaria para la ejecución de un contrato** entre el interesado y el responsable del tratamiento.
  - Necesaria por razones importantes de interés público.
  - La transferencia es requerida para la formulación, el ejercicio o la defensa de reclamaciones.
  - Necesaria para proteger los **intereses vitales** del interesado o de otras personas.
  - La transferencia se efectúa desde un registro público, destinado a facilitar información al público en general.

Además, si no es aplicable nada de lo anterior, se introduce una excepción, aplicable para las transferencias de datos, en los casos en que estas sean esporádicas, no repetitivas y para satisfacer de manera urgente el interés legítimo del responsable de tratamiento, siempre y cuando, como ya hemos visto con relación al interés legítimo, este prevalezca sobre los derechos y libertades de los afectados; y además debe ser notificada a las autoridades de control.

Ideas clave

Acuerdos

La UE y EE. UU. han buscado en los últimos 25 años mecanismos para salvar las diferencias regulatorias y facilitar las transferencias internacionales de datos de la UE hacia EE. UU. mediante acuerdos bilaterales. Primero fue el acuerdo Safe Harbor, al que le sucedió, tras su anulación en 2015, el acuerdo Privacy Shield, que también ha sido anulado, en julio de 2020, por el Tribunal de Justicia de la Unión Europea (TJUE).

Al cierre de este temario, para las transferencias internacionales de datos desde UE a los EE. UU., hay que tener en consideración que:

EE. UU. no goza de ningún acuerdo específico, por lo que debe regirse por los principios de la transferencia internacional de datos a cualquier país fuera de la UE y que no cuente con una decisión de adecuación de la Comisión.

8.11. Seguridad de la información y protección de datos

Como sabemos, la seguridad es uno de los principios fundamentales de la protección de datos personales, y así se contempla en el RGPD.

Los datos serán «tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad")» (art. 5.1, RGPD).

Objetivos alineados con la definición de la seguridad de la información que hacen los principales estándares de la materia:

- **Seguridad de la información:** «preservación de la confidencialidad, integridad y disponibilidad de la información» (ISO/IEC 27000:2014).

Término al que también es habitual asociar otras propiedades como son autenticidad, responsabilidad, *accountabilty,* no repudiación o confiabilidad.

Hay que remarcar que **sin seguridad no sería posible garantizar la privacidad de los datos personales ni los derechos y libertades de los ciudadanos.** Ahora bien, la seguridad es un camino en búsqueda de un concepto absoluto, pero imposible de alcanzar, cual paradoja de Zenón.

La seguridad absoluta no existe. Se abordan los riesgos sobre la disponibilidad, integridad y confidencialidad aplicando medidas técnicas y organizativas, con objeto de mitigarlos, transferirlos o aceptarlos; buscando el equilibrio entre el coste de las medidas y su efecto sobre los riesgos.

Por ello es fundamental entender que la seguridad debe ser un proceso gestionado y continuo, orientado a la mejora continua, un ciclo de Deming, más conocido como PDCA (planificar-hacer-verificar-actuar permanentemente), destinado a dotar a los tratamientos de datos de carácter personal del entorno de seguridad adecuado y robusto para minimizar los riesgos sobre las personas.

El RGPD integra la seguridad dentro de las obligaciones de **responsabilidad proactiva,** tanto de responsables de tratamiento como de encargados de tratamiento. No detalla un conjunto de medidas de seguridad, específicamente establecidas, aunque el reglamento contempla aproximaciones que pueden ayudar a las organizaciones a demostrar su alineamiento con la responsabilidad exigida en el RGPD, como son las certificaciones y los códigos de conducta.

Aunque el RGPD prevé el desarrollo por parte de la autoridad de control de la especificación de medidas concretas de seguridad aplicables a escenarios de riesgo de tratamiento de datos personales específicos.

El RGPD incorpora una aproximación a la seguridad desde la responsabilidad exigible, superando las aproximaciones tuteladas por las autoridades previas al RGPD.

Este tutelaje por parte de la autoridad se mostraba de forma clara en el marco legislativo español, que ha incorporado un conjunto de medidas de seguridad concretas para aplicar a los tratamientos, medidas que eran obligatorias y con carácter de mínimos requeridos. El RD 1720/2007 (derogado) clasificaba las medidas de seguridad que aplicar en función de tres niveles de seguridad diferenciados y que se establecen en función del tipo de datos de carácter personal (DCP) manejados (art. 81, RDLOPD).

En España, estos reglamentos fueron una oportunidad para **promover el concepto de seguridad de la información** entre empresas y organizaciones.

De hecho, en el mundo de la mediana y pequeña empresa, donde la concienciación en seguridad era realmente baja, de la mano de las adaptaciones a la normativa en protección de datos personales se fueron incorporando conceptos como: uso de contraseñas, realización de copias de seguridad, personal autorizado, etc. Se introducían medidas de seguridad en las organizaciones para dar respuesta a una obligación y se beneficiaban las empresas al incluir dentro del dominio de aplicación de las medidas información vital para las empresas: clientes, RR. HH., etc. Seguramente, esto fue posible por la concreción de controles y medidas de seguridad.

Buenas prácticas en la seguridad de la información

En estos años se han venido desarrollando formalmente conjuntos de buenas prácticas para la gestión de la seguridad de la información, alcanzando una madurez significativa y cuya aproximación a la seguridad siempre se basa en el riesgo y en la eficacia de los controles de seguridad en su reducción.

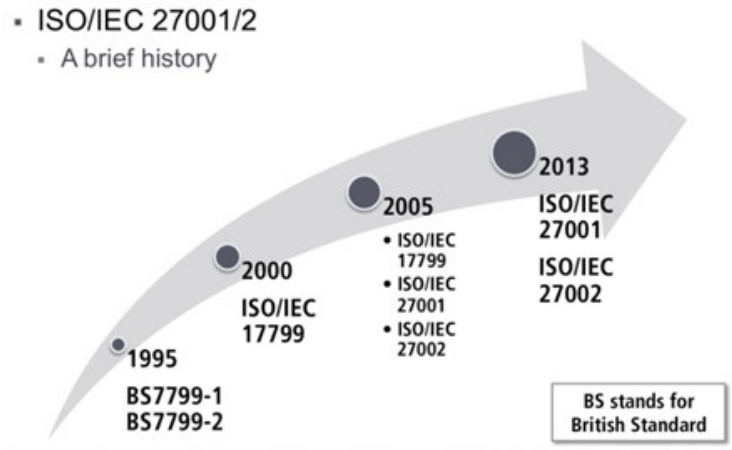
Entre los numerosos marcos existentes, a título informativo tenemos:

- NIST. Las normas de seguridad del National Institute of Standars and Technology de EE. UU. Establece las bases de seguridad de las AA. PP. e integra publicaciones.
- Serie ISO/IEC 27000. Integra, entre otras, la conocida norma ISO/IEC 27001:2013 (Information technology. Security techniques. Information security management systems. Requirements).
- COBIT 2019. Marco de referencia para la gestión integral del gobierno de las TI en las organizaciones que incluye la seguridad de la información. Desarrollado por ISACA.

- Common Criteria (ISO/IEC 15408). Orientada a la armonización de los requisitos de seguridad de productos de *hardware, software, firmware*.

- ENS: Esquema Nacional de Seguridad. Ofrece un marco de seguridad para las administraciones públicas españolas.

ISO/IEC 27001



Veamos con un poco más de detenimiento la ISO/IEC 27001.

Figura 9. Breve historia ISO/IEC 270001. Fuente: Martins, 2018.

Consolida más de 18 años de trabajo en el desarrollo del estándar cuyos orígenes son desarrollados por British Standard Institution (BSI).

Establece el marco de referencia para un sistema de gestión de la seguridad de la información (SGSI) y es certificable IEC/ISO 27001:2013 (Information technology. Security techniques. Information security management systems. Requirements) y la norma ISO/IEC 27002:2013 (Information technology. Security techniques. Code of practice for information security controls) incorporaba un marco de buenas prácticas de controles de seguridad de la información.

Ideas clave

Las dos normas forman parte de la serie ISO/IEC 27000, que desarrolla controles de seguridad, metodologías de evaluación de riesgos, etc. Es decir, desarrolla un marco de gestión de la seguridad de la información, que además es certificable.

Para familiarizarnos con los controles de seguridad que habitualmente se deben disponer en las organizaciones para salvaguardar los activos de información, nos introducimos brevemente en la norma de seguridad ISO/IEC 27002.

La ISO/IEC 27002 **incorpora 14 dominios de seguridad, sobre los que identifica 35 objetivos de control de seguridad, con un total de 114 controles de seguridad.**

En el siguiente esquema se recogen los dominios de seguridad y los objetivos de control de la norma.

Ideas clave

ISO/IEC 27001	5. Políticas de seguridad de las organizaciones.
	6. Aspectos organizativos de los sistemas de información.
	7. Recursos humanos.
	8. Gestión de activos de información.
	9. Control de acceso a la información.
	10. Cifrado.
	11. Seguridad física y del entorno.
	12. Seguridad de la operativa.
	13. Telecomunicaciones.
	14. Adquisición, desarrollo y mantenimiento de los sistemas de información.
	15. Suministradores.
	16. Gestión de incidentes.
	17. Continuidad de negocio.
	18. Cumplimiento.

Nota: en la Biblioteca virtual de UNIR al cierre de este tema se dispone de acceso a la biblioteca AENOR, donde está disponible la UNE-EN ISO/IEC 27001:2017 (con origen en la ISO/IEC 27001:2013).

8.12. Referencias bibliográficas

AEPD. (s.f.). Guía para el cumplimiento del deber de informar. https://www.aepd.es/es/documento/guia-modelo-clausula-informativa.pdf-0

Avram, R., Daoud, S., y Atme, J. (2020). Oracle public cloud [Diapositivas]. *Oracle.* https://clubutilisateursoracle.org/wp-content/uploads/2020/09/AUFO_Cycle_Securite_Session_2_Oracle_220920.pdf

Brandon, H., y de Souza, L. (2016). *Big Data Analytics and privacy & data protection.* Atos Codex. https://atos.net/wp-content/uploads/2017/01/atos-big-data-analytics-privacy-data-protection-whitepaper.pdf

Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de las Comunidades Europeas C 364, 18 de diciembre de 2000, pp. 1-22. https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Hoskins, M. (18 octubre de 2012). Hooray - more data protection compliance diagrams [Mensaje en un blog]. *Blogger.* http://dataprotector.blogspot.com/2012/10/hooray-more-data-protection-compliance.html

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281, pp. 33987-34058. https://www.boe.es/eli/es/lo/1995/11/23/10/con

Martins, M. (2018). Information Security Strategic Management [Diapositivas]. *Speaker Deck.* https://speakerdeck.com/mmartins000/information-security-strategic-management

Real Academia Española. (2020). Leal. En *Diccionario de la lengua española* (23a ed.).

https://dle.rae.es/leal

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). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 1-88.

https://www.boe.es/doue/2016/119/L00001-00088.pdf

Agencia Española de Protección de Datos

AEPD. Página web oficial. https://www.aepd.es/es

Encontrarás preguntas frecuentes, documentación de soporte e información sobre procedimientos sancionadores.

Comisión Europea

Comisión Europea. (s.f.). Protección de datos [Página web]. https://ec.europa.eu/info/law/law-topic/data-protection_es

En esta página encontrarás información sobre la Comisión Europea para el nuevo Reglamento de Protección de Datos.

Hacia un nuevo modelo europeo de protección de datos

Piñar, J. L. (dir.) (2007). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos.* Reus.

Profundo análisis sobre cada uno de los aspectos relevantes del nuevo marco europeo de protección de datos. Una extensa guía de referencia.

Test

1. De entre los siguientes, ¿cuáles tienen la consideración de datos de carácter personal por parte del RGPD?

A. Un nombre.

B. Un número de identificación.

C. Información genética.

D. Todos los anteriores.

2. De entre los siguientes datos, ¿cuáles no tienen la consideración de datos de categorías especiales?

A. Las opiniones políticas.

B. Los datos de ingresos mensuales.

C. Los tratamientos de datos genéticos.

D. Los datos relativos a la salud de las personas.

3. Cuando nuestros datos de carácter personal se quieren incorporar a un tratamiento por una organización, está obligada a:

A. Informar sobre quién o quiénes son los responsables del tratamiento.

B. Informar sobre la finalidad por la que recaban los datos y se van a realizar los tratamientos.

C. Informar si procede de los destinatarios o grupos de destinatarios de las comunicaciones de datos que se vayan a efectuar.

D. Todas las respuestas anteriores son ciertas.

4. De las operaciones siguientes, indica cuáles se consideran tratamiento de datos:

A. Recogida de datos de clientes en un formulario *online.*

B. Conservación de datos en copias de seguridad.

C. Consulta de datos de forma telemática.

D. Todas las respuestas anteriores son ciertas.

5. De entre los siguientes, indica cuáles son principios de la protección de datos conforme al RGPD.

A. Minimización de datos.

B. Exactitud de los datos.

C. Responsabilidad proactiva.

D. Todos los anteriores.

6. De entre los siguientes, indica cuáles son obligaciones del responsable de tratamiento conforme al RGPD.

A. Atender a las autoridades de control.

B. Notificar las fallas de seguridad a las autoridades de control y afectados, cuando sea preciso.

C. Seleccionar diligentemente y formalizar la relación con los encargados de tratamiento.

D. Todas las anteriores.

7. Respecto a las transferencias internacionales a EE. UU., indica qué afirmación es cierta:

A. Si existe el consentimiento del afectado, se puede realizar dicha transferencia.

B. Si EE. UU. dispone de una decisión de adecuación de la Comisión que reconoce un nivel de protección en materia de protección de datos equivalente al de la UE.

C. Las organizaciones de EE. UU. certificadas de acuerdo con el Escudo de Privacidad (Privacy Shield) tienen reconocido un nivel de protección equivalente al de la UE.

D. En ningún caso se pueden transferir datos a organizaciones residentes en EE. UU.

8. Indica qué afirmación es verdadera:

A. Las legislaciones en protección de datos de EE. UU. y la UE son legislaciones tipo ómnibus y equivalentes.

B. La exportación de datos desde la UE a EE. UU. es libre.

C. A nivel internacional, la mayoría de los países ofrecen un nivel fuerte de protección en materia de protección de datos equivalente al de la UE.

D. Existe disparidad entre los marcos legales de la UE y de EE. UU.

9. Las trasferencias internacionales de datos son una práctica habitual, pero ¿son legales?

A. Sí, siempre que el usuario adecuadamente informado consienta a la transferencia.

B. Sí, cuando es necesaria para ejecutar un contrato entre el afectado y el responsable del tratamiento.

C. Sí, si existe una decisión de la Comisión que reconoce, sobre el país destinatario, un nivel de protección equivalente al de la UE.

D. En todos los casos anteriores son legales.

10. Respecto a los derechos que el RGPD reconoce a los afectados, ¿cuál de entre los siguientes no es cierto?

A. Acceso.

B. Rectificación.

C. Oposición.

D. Legitimación.