ANÁLISIS DEL REGLAMENTO EUROPEO 2016/679, DE PROTECCIÓN DE DATOS*

Iuliana Raluca Stroie**
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 13 de julio de 2018

1. Introducción

El Reglamento (UE) 2016/679 de protección de datos que entró en vigor el 24 de mayo de 2016 empezó a aplicarse el pasado 25 de mayo de 2018 sustituyendo a la Directiva 95/46/CE, sobre protección de datos, y a la Directiva (UE) 2016/680 sobre cooperación policial. Aunque se trate de un conjunto de normas directamente aplicables, que se basa en la normativa vigente de los distintos Estados miembros de la UE, también contiene una serie de novedades que se repercuten en distintos ámbitos. Es por ello por lo que se dejó un plazo de dos años entre la fecha de su entrada en vigor y la de aplicación, para que tanto los Estados miembros como las partes interesadas pudiesen llevar a cabo la labor de adaptación para su aplicación. Los Estados miembros tenían la obligación de adaptar su legislación mediante la derogación y modificación de las leyes existentes, implantar autoridades nacionales de protección de datos, elegir un organismo de acreditación y establecer las normas para la conciliación de la libertad de expresión y la protección de los datos. No obstante, en enero de 2018 sólo dos de los 27 Estados miembros habían adaptado su legislación nacional estando los demás en distintas etapas de adaptación.

2. Objeto y ámbito de aplicación

A lo largo de sus 99 artículos estructurados en 11 capítulos, el Reglamento contiene unas disposiciones generales, enumera los principios relativos al tratamiento de datos personales, regula los derechos del interesado, la figura del responsable, el encargado del tratamiento, el delegado y la autoridad de control, las transferencias de datos personales

* Trabajo realizado en el marco del Proyecto Convenio de colaboración entre la UCLM y el Ilustre Colegio Notarial De Castilla-La Mancha (17 enero 2014) (OBSV) con referencia CONV140025, que dirige el Prof. Ángel Carrasco Perera
** ORCID ID: 0000-0003-1998-5412

a terceros países u organizaciones internacionales, establece las normas relativas a la cooperación y coherencia, los recursos, responsabilidad y sanciones, y las disposiciones relativas a situaciones específicas de tratamiento y actos de ejecución.

El objetivo de la norma es la protección de los derechos y libertades fundamentales de las personas físicas, en particular, el derecho a la protección de los datos personales y también la regulación de la circulación de esos datos.

Desde un punto de vista material, la norma resulta de aplicación "al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero[1]". Quedan excluidas, conforme se señala en el art. 2.2., las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, las actividades de los Estados miembros relacionadas con la política exterior y la seguridad común de la UE, el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas y, las actividades llevadas a cabo por las autoridades competentes en relación a la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales.

Desde el punto de vista territorial, el Reglamento amplía su ámbito de aplicación. Así, este resultará aplicable en el espacio europeo, y también fuera de ese ámbito si el responsable o encargado de las actividades de tratamiento de datos no está establecido en la Unión y estas están relacionadas con la oferta de bienes o servicios a interesados residentes en la Unión y el control de su comportamiento tiene lugar en la Unión, o bien el responsable está establecido en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

3. Principios aplicables al tratamiento de datos

Algunos de los principios contenido en el Capítulo II ya venían recogidos en la normativa anterior, no obstante, el Reglamento los desarrolla incorporando algunos elementos nuevos y, además, incorpora *ex novo* una serie de principios con la finalidad de reforzar la protección de los derechos de las personas y la libre circulación de los datos.

Así, además de los principios relativos a la licitud, lealtad y transparencia, exactitud, limitación de la finalidad, minimización de datos, limitación del plazo de conservación se introducen principios relativos a la integridad y confidencialidad y responsabilidad proactiva del responsable del tratamiento de datos.

[1] Conforme se señala en el art. 2.1 del Reglamento.

3.1. Licitud del tratamiento de datos personales

Conforme al art. 6 del Reglamento, el tratamiento será licito si el interesado dio su consentimiento, si se haya firmado algún contrato o documento precontractual, si el responsable está habilitado por una disposición legal, si se trata de proteger intereses vitales del interesado o de otra persona física, el interés público o, intereses legítimos del responsable del tratamiento o de un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado. Estos requisitos no se deben cumplir de forma cumulativa, sino que se trata de unos requisitos alternativos, recayendo en el responsable del tratamiento la obligación de demonstrar que se ha cumplido alguno de ellos.

Una de las novedades introducidas por el Reglamento, relativa al principio de licitud, se refiere a la forma de recabar el consentimiento del interesado. Si en la Ley de 1999 se admitía el consentimiento tácito, el Reglamento excluye esta posibilidad, delimitando las condiciones en las que se ha de recabar en el art. 4. 11). Así, el consentimiento deberá expresarse de forma inequívoca, es decir, se requiere una afirmación o acción positiva por parte del interesado que demuestre su conformidad y en algunos casos, conforme se señala en la Guía publicada por la AEPD[2], para el tratamiento de datos sensibles[3], adopción de decisiones automatizadas y transferencias internacionales, tendrá que ser explicito[4].

En su art. 9.1, el Reglamento prohíbe con carácter general el tratamiento de los datos sensibles, prohibición que podrá ser levantada solo si se cumple alguno de los requisitos enumerados en el apartado 2 del mismo artículo[5].

[2] http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf#Gu%C3%ADa%20del%20Reglamento%20General%20de%20Protecci%C3%B3n%20de%20Datos%20para%20responsables%20de%20tratamiento

[3] El Reglamento amplía el listado de datos sensibles introduciendo, además de aquellos que hacen referencia al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, a los relativos al tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

[4] La AEPD aclara que "El consentimiento puede ser inequívoco y otorgarse de forma implícita cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación)".

[5] Conforme al art. 9.2. del Reglamento, es posible el tratamiento de datos especiales cuando:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que

Además, el consentimiento podrá ser revocado en cualquier momento, aunque se haya recabado de forma licita.

Conforme al Considerando 171 del Reglamento, el consentimiento recabado de conformidad a la Directiva 95/46/CE y que cumpla los requisitos de aquél es válido y el responsable puede continuar el tratamiento de los datos con posterioridad a su fecha de aplicación sin necesidad de recabar de nuevo el consentimiento. Por tanto, solo servirá aquel consentimiento recabado con anterioridad a la fecha de aplicación del Reglamento si este ha sido expresado mediante una acción o manifestación afirmativa por parte del interesado.

En relación al tratamiento de datos de los menores de edad, la LOPD permite recabar los datos del menor de 14 años sin necesidad del consentimiento de los padres. El

establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c)el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d)el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i)el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Reglamento eleva dicha edad a 16 años, no obstante, permite que las leyes nacionales establezcan una edad inferior que, en ningún caso, será menos de 13 años.

3.2. Principio de limitación de la finalidad

Una de las novedades introducidas por el Reglamento se refiere al principio de limitación de la finalidad, conforme al cual, los datos serán recogidos para fines determinados, explícitos y legítimos y no serán tratados posteriormente de manera incompatible con dichos fines. No obstante, conforme al artículo 89 apartado 1, 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.

3.3. Principio de transparencia

El principio de transparencia al que se refiere el art.5.1 debe relacionarse con el derecho a la información del interesado recogido en el art. 12 del Reglamento. El responsable del tratamiento está obligado a facilitar al interesado toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Se admite facilitar la información de forma verbal solo si el interesado así lo ha solicitado pero el responsable deberá poder demonstrar la identidad de aquél por otros medios. La información que se ha de facilitar al interesado versa sobre la existencia del fichero o tratamiento, su finalidad y destinatarios, el carácter obligatorio o no de la respuesta, así como de sus consecuencias, la posibilidad de ejercitar los derechos de acceso, rectificación o supresión y, la identidad y datos de contacto del responsable del tratamiento. El Reglamento, añade a los anteriores requisitos los datos de contacto del Delegado de Protección de Datos, la base jurídica o legitimación para el tratamiento, el plazo o los criterios de conservación de la información, la existencia de decisiones automatizadas o elaboración de perfiles, la previsión de transferencias a terceros países, el derecho a presentar una reclamación ante las autoridades de control y además, en el caso de que los datos no se obtengan del propio interesado se ha de informar sobre el origen y las categorías de los mismos.

El responsable deberá facilitar la información anterior en el momento en que se soliciten los datos o previamente a la recogida o registro, si los datos se obtienen directamente del interesado. Si los datos no se obtienen directamente del interesado, la información se debe facilitar antes de un mes desde que se obtuvieron los datos personales, antes o en la primera comunicación con el interesado, o antes de que los datos se hayan comunicado a otros destinatarios.

Conforme a lo dispuesto en el art. 13.5., se exime al responsable de la obligación de informar cuando el interesado ya disponga de la información, o, en el caso de que los datos no procedan del interesado, cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado, el registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros, o cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

3.4. Principio de "minimización de datos"

El artículo 5.1.c) establece que "los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Este principio, sustituye al principio de calidad de datos de la LOPD y debe ser relacionado con el principio de protección de datos desde el diseño y por defecto recogido en el art. 25 del Reglamento. Básicamente se refiere a la obligación del responsable de tratamiento de reducir al máximo la cantidad de datos tratados, la extensión de su tratamiento y el plazo de conservación y accesibilidad.

Asimismo, se recoge la obligación del responsable de aplicar "las medidas técnicas y organizativas apropiadas" para garantizar que, "por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento". Dichas medidas deben garantizar que, "por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas" lo que significa por ejemplo que un perfil de Facebook que por defecto era visible para cualquier usuario de dicha red social ahora lo será solo si el titular del mismo lo haga accesible para aquellos. Se pretende por tanto, mediante el principio de *Privacy by Design*, devolver al usuario el control sobre su privacidad.

Se trata en definitiva de una obligación de los responsables del tratamiento de prevenir de forma activa los riesgos que entraña el tratamiento de datos personales, mediante el diseño de tecnologías que permitan identificarlos y prevenirlos antes de que se conviertan en daños para el titular de los datos.

3.5. Principio de "exactitud"

Este principio, recogido en el art. 5.1 d) requiere al responsable que los datos tratados sean exactos y si fuera necesario actualizados, para lo que deberá adoptar las medidas necesarias para comprobar la veracidad de los mismos y suprimir o rectificar aquellos que sean inexactos para los fines para los que se tratan.

3.6. Principio de limitación del plazo de conservación

Conforme a este principio, los datos que permiten la identificación del titular no deben ser mantenidos más tiempo del necesario para los fines del tratamiento. Al igual que en el caso del principio de limitación de la finalidad, se considerará justificado el tratamiento prolongado si el fin es de archivo en interés público, de investigación científica o histórica o estadísticos, conforme al artículo 89, apartado 1.

3.7. Principio de integridad y confidencialidad

A través de este principio se impone la obligación a los responsables del tratamiento de utilizar las medidas técnicas u organizativas apropiadas para garantizar la seguridad de los datos que incluya la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

3.8. Principio de responsabilidad proactiva

Por último, el art. 5.2 recoge la obligación de los responsables de cumplir los principios recogidos en el apartado 1 y de demonstrar su cumplimiento. Para ello, conforme se señala en el Considerando 74 del Reglamento, el responsable debe aplicar medidas oportunas y eficaces, poder demostrar la conformidad de las actividades de tratamiento con lo contenido en el Reglamento, así como la eficacia de las medidas adoptadas.

4. Derechos del interesado

Los derechos del interesado están recogidos en los arts. 12 al 22 del Reglamento. Algunos de ellos al estar directamente relacionados con los principios antes analizados han sido mencionados en los párrafos anteriores, como por ejemplo el derecho a la información, recogido en el art. 12 y desarrollado en los arts. 13 y 14.

4.1. Derecho de acceso

El interesado tiene derecho a "obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales" (art. 15). La información que se ha de facilitar al interesado en cumplimiento de su derecho de acceso se refiere a: a) los fines del

tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Conforme al art. 15.2 el interesado tiene derecho a recibir información relativa a los datos que se transfieren a un tercer país o a una organización internacional, en un formato accesible y legible de modo que aquel pueda entender cuales son los datos que se transfieren.

El cumplimiento de la obligación del responsable, de facilitar la información antes mencionada, se realiza mediante el envío al interesado de una copia de los datos tratados. La información podrá ser facilitada por medios electrónicos si la solicitud del interesado se ha realizado a través de estos medios y no ha especificado que se facilite de otro modo, en el plazo máximo de un mes desde la solicitud (Considerando 59). Además, se prevé la gratuidad para la primera copia y la posibilidad que tiene el responsable de cobrar un canon basado en costes administrativos.

4.2. Derechos de rectificación y supresión («el derecho al olvido»)

Los arts. 16 y 17 del Reglamento regulan el derecho a la rectificación y el derecho a la supresión de datos del interesado. Así, el derecho de rectificación, que no es otra cosa que la materialización del principio de exactitud recogido en el art. 5.1 d), obliga al responsable a garantizar que los datos sean exactos y actualizados. El interesado puede solicitar la rectificación, en su caso que se completen sus datos, y el responsable deberá dar curso a dicha solicitud sin dilación indebida y a más tardar en el plazo de un mes.

El derecho de supresión, recogido en el art. 17, es el derecho que asiste al interesado de exigirle al responsable que suprima el tratamiento de sus datos personales si ya no son necesarios para el fin para el que fueron recogidos, por no mantener su

consentimiento y el fundamento del tratamiento no se base en un contrato o previsión legal o, si los datos han sido tratados de forma ilícita.

No obstante, el derecho de supresión que asiste al interesado debe considerarse sin perjuicio de la obligación del responsable de suprimir el tratamiento conforme al principio de responsabilidad proactiva contenida en el art. 5.2 si desaparece cualquiera de las condiciones del art. 6.1 que regula la licitud del tratamiento o se incumple alguno de los principios recogidos en el art. 5.1.

Por otro lado, para reforzar el cumplimiento del «derecho al olvido», el responsable está obligado a indicar a los responsables que tratan replicas o copias de los datos a suprimir cualquier enlace, copias o réplicas de los datos. Para ello, el responsable debe utilizar las medidas técnicas razonables para informar a los responsables de la solicitud del interesado. Por tanto, conforme se señala en el Considerando 66 del Reglamento, el derecho al olvido no se puede confundir o identificar con el derecho de supresión, sino que aquel se configura como una ampliación o extensión del derecho de supresión.

No obstante, los derechos de supresión y al olvido no son derechos absolutos ya que en el apartado tercero del art. 16, se recogen algunas excepciones a los mismos. Así, los derechos antes mencionados devienen inoperables frente al derecho de libertad de expresión e información. Tampoco tendrán preferencia si se trata del cumplimiento de una obligación legal que requiera el tratamiento de datos, del interés público en el ámbito de la salud pública, de fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en la que la supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento y por último, si se requiere el tratamiento de los datos para la formulación, el ejercicio o la defensa de reclamaciones.

4.3. Derecho a la limitación del tratamiento

El interesado también tiene derecho a solicitar la limitación del tratamiento de sus datos personales en el futuro si: i) impugna la exactitud de los mismos para el plazo que permita al responsable verificar la exactitud de los mismos; ii) el tratamiento es ilícito y el interesado se opone a la supresión solicitando en su lugar la limitación de su uso; iii) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones y, iv) el interesado se haya opuesto al tratamiento en virtud de su derecho a oposición, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. Para llevar a cabo la suspensión temporal del tratamiento, el responsable puede trasladar temporalmente los datos

seleccionados a otro sistema de tratamiento, impedir el acceso de usuarios a los datos personales seleccionados o de retirar temporalmente los datos publicados de un sitio internet.

Teniendo en cuenta que en el caso de tratamiento ilícito el responsable, en base al principio de responsabilidad proactiva, debería suprimir el tratamiento, y que el interesado puede sustituir dicha supresión por la limitación del tratamiento, se puede concluir que para este caso, el responsable no tiene la obligación derivada del principio de responsabilidad proactiva y la limitación sólo se puede conseguir ante la previa solicitud del interesado.

En todo caso, el responsable tiene la obligación de informar al interesado antes de efectuar el levantamiento de la limitación. Asimismo, los datos no podrán volver a ser tratados sin el consentimiento del interesado salvo que se trate de su conservación o se requiera su tratamiento para la formulación, el ejercicio o la defensa de reclamaciones, para la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la UE o de un determinado Estado miembro.

4.4. Derecho de portabilidad

El derecho de portabilidad se refiere al derecho del interesado de recibir los datos personales que le incumban y haya facilitado a un responsable del tratamiento y de transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado inicialmente (art. 20).

Para que se pueda ejercer el derecho de portabilidad se deben cumplir los siguientes requisitos de forma cumulativa. En primer lugar, los datos tienen que ser de la persona que haya solicitado la portabilidad, es decir el responsable tendrá que comprobar la veracidad de los mismos. Además, se requiere que los datos hayan sido facilitados por el interesado y tratados en base al consentimiento otorgado de conformidad al art. 6.1 a) o al consentimiento explícito si se trata de categorías especiales de datos y su tratamiento no está prohibido mediante norma imperativa de la UE o algún Estado miembro, o, que se hayan facilitado como consecuencia de la celebración de un contrato. Por último, se requiere que los datos sean tratados por medios automatizados.

La entrega de los datos se puede realizar bien al mismo interesado o bien directamente al otro responsable en el plazo de un mes desde la solicitud. En todo caso, el responsable tiene la obligación de facilitarlos en un formato estructurado, de uso común y lectura mecánica y en formato que sea interoperable.

4.5. Derecho de oposición

Como se desprende de los párrafos anteriores, los derechos del interesado pueden sufrir limitaciones si la finalidad del tratamiento se refiere al interés público u otros intereses legítimos del responsable. Para estos últimos casos, la norma europea regula el derecho de oposición del interesado en su art. 21. Concretamente, el interesado tendrá derecho a oponerse al tratamiento de sus datos personales si este resulta necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable o, si resulta necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero. Además, el interesado tendrá derecho a oponerse al tratamiento de sus datos cuando dicho tratamiento tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. Por último, basándose en motivos relacionados con su situación particular, el interesado podrá oponerse al tratamiento de datos con fines de investigación científica o histórica o fines estadísticos, salvo que dicho tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Si el tratamiento se realiza a través de servicios de la sociedad de la información el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

Para garantizar la eficacia del derecho de oposición, la norma impone al responsable la obligación de informar de manera explícita y clara al interesado y al margen de cualquier otra información acerca de su derecho, a más tardar en el momento de la primera comunicación. Como consecuencia del ejercicio del mentado derecho, el responsable dejará de tratar los datos siempre y cuando no pueda acreditar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

4.6. Decisiones individuales automatizadas, incluida la elaboración de perfiles

El derecho del interesado conforme al cual sus datos personales no sean objeto de un tratamiento basado exclusivamente en una decisión automatizada, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, cierra el listado de los derechos contenidos en el Capítulo III del Reglamento. Es notorio que el avance tecnológico de la era digital ha hecho posible la recopilación, conservación y tratamiento de datos personales

totalmente de forma automatizada, sin que medie intervención humana. A través de estos procedimientos se realizan estudios automáticos basados en circunstancias concretas del individuo como por ejemplo, sus preferencias o intereses personales, su situación económica, aspectos relativos a rendimientos de trabajo o la salud, que pueden ser aplicados a casos posteriores y generar consecuencias, que podrían ser distintas en caso de obrar la intervención humana en la toma de decisiones.

Por tanto, si bien el Reglamento permite que el interesado esté sometido a una decisión automatizada, como consecuencia del tratamiento de sus datos personales, le otorga a este el derecho de oponerse a la misma, salvo que sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, haya otorgado su consentimiento explícito o, está autorizada por el Derecho de la Unión o de los Estados miembros, siempre y cuando se establezcan las medidas adecuadas para salvaguardar los derechos, las libertades y los intereses legítimos del interesado.

No obstante, se prevé como regla general la prohibición de someter al interesado a una decisión automatizada si el tratamiento se refiere a categorías de datos personales sensibles, salvo que el interesado haya prestado su consentimiento explícito para el tratamiento de dichos datos con uno o más de los fines especificados y no exista una norma imperativa que limite su derecho de disposición sobre esos datos o, el tratamiento sea necesario por razones de un interés público esencial basado en el Derecho de la UE o los Estados miembros.

5. Limitaciones a los derechos del interesado

Mediante el art. 23 del Reglamento se otorga a los Estados miembros la facultad de establecer limitaciones a la eficacia de los derechos anteriormente analizados siempre y cuando con dichas limitaciones se persigue salvaguardar:

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;
h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);
i) la protección del interesado o de los derechos y libertades de otros;
j) la ejecución de demandas civiles.

6. El responsable y el encargado del tratamiento de datos

Conforme al art. 4.7) el responsable del tratamiento es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento". En el párrafo octavo del art. 4 se define el concepto de encargado como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

Como ya se ha podido observar, al analizar los principios y distintos derechos del interesado, el responsable tiene la responsabilidad por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. Para cumplir con este deber, el responsable debe analizar los riesgos, la naturaleza, ámbito, contexto y el fin del tratamiento y, aplicar las medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Además, tiene la obligación de revisar y actualizar dichas medidas cuando sea necesario.

El Reglamento no contiene una lista exhaustiva de las medidas de seguridad técnicas u organizativas, no obstante, a lo largo de su articulado, establece una serie de medidas, como por ejemplo, las de protección de datos desde el diseño, las de protección por defecto, de información al interesado, etc. e indica en el art. 32 que para la seguridad del tratamiento, el responsable podrá aplicar, entre otras medidas la seudonimización y el cifrado de datos personales. Además, señala que las medidas adoptadas pueden incluir la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, y por último, un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Es importante señalar que el Reglamento condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. Para ello establece dos niveles de riesgos señalando que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertades de los interesados

mientras que en otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve. En consecuencia, los responsables tienen la obligación de analizar los riesgos teniendo en cuenta los tipos de tratamiento, la naturaleza de los datos, el número de interesados afectados y la cantidad y variedad de tratamientos que una misma organización lleve a cabo. Si se trata de grandes organizaciones el análisis deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo existentes. Por el contrario, si se trata de organizaciones pequeñas y con tratamientos de poca complejidad, el análisis será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados. Concretamente, lo que se debe valorar en este último caso es si se tratan datos sensibles, si se incluyen datos de una gran cantidad de personas, si el tratamiento incluye la elaboración de perfiles, si se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes, si se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades, si se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data, y por último, si se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas. Solo si la valoración de estas cuestiones resulta negativa será razonable concluir que la organización no realiza tratamientos que generen un elevado nivel de riesgo y que, por tanto, no debe poner en marcha las medidas previstas para aquellos casos.

Asimismo, el Considerando 77 prevé que el Comité puede aprobar códigos de buenas prácticas, certificaciones o directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento.

En virtud del principio de responsabilidad proactiva, el responsable tiene la obligación de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento. Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados. Para demostrar que los encargados o subencargados ofrecen las garantías exigidas por la nueva norma, éstos podrán adherirse a códigos de conducta o certificarse dentro de los esquemas previstos por el Reglamento.

El tratamiento llevado a cabo por el encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión (apartados 6, 7 y 8 del art. 28). Una vez finalizado el

tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos. Por tanto, la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad.

No obstante, si bien la normativa anterior se centraba en la actividad del responsable, el Reglamento contiene obligaciones expresamente dirigidas a los encargados como por ejemplo mantener un registro de actividades de tratamiento, determinar las medidas de seguridad aplicables a los tratamientos que realizan o, designar a un Delegado de Protección de Datos en los casos previstos por el Reglamento y que no estén recogidos en los contratos.

7. El Delegado de Protección de Datos

El Reglamento regula en la Sección cuarta del Capitulo IV la figura del Delegado de Protección de Datos. Si bien el Reglamento no define el concepto en su art. 4, el Considerando 97 indica que será una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos. Las personas que han de designar al delegado serán el responsable o el encargado del tratamiento, pero la designación se requiere solo para determinados casos:

1º Si el tratamiento lo llevan a cabo autoridades y organismos públicos a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial.

2º Si los responsables o encargados tienen entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala

3º Si los responsables o encargados tienen entre sus actividades principales el tratamiento a gran escala de datos sensibles

Para los demás casos, el responsable o encargado podrán designar un delegado si así lo desean, pero la obligación de hacerlo no recae sobre ellos.

El nivel de conocimientos del delegado debe determinarse en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado.

El delegado podrá formar parte o no de la plantilla del responsable, pero su independencia no puede verse afectada por este hecho. La designación del delegado y sus datos deben comunicarse a las autoridades de control competentes.

El Reglamento establece algunas obligaciones respecto a la relación entre delegado y responsable o encargado del tratamiento. Así, el responsable y el encargado deben garantizar que el delegado pueda participar de forma adecuada en las cuestiones relativas a la protección de datos, y que este no recibirá indicación alguna y tampoco podrá ser destituido o sancionado respecto al desempeño de sus funciones. Por su parte, el delegado estará obligado a mantener el secreto o la confidencialidad y rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Las funciones del delegado están recogidas en el art. 39 y son las siguientes:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;
d) cooperar con la autoridad de control;
e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

8. Códigos de conducta y certificaciones

Conforme al art. 40.1, los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta a los que los responsables o encargados podrán adherirse para demostrar el cumplimiento de lo dispuesto en el Reglamento. Estos serán elaborados por las asociaciones u otros organismos que representen a categorías de responsables o encargados con el fin de facilitar su aplicación efectiva y teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. A través de los códigos de conducta se podrán establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que el tratamiento de datos pueda acarrear. Para su elaboración se han de consultar las partes interesadas, incluidos los interesados, cuando sea posible.

La aprobación de los códigos de conducta la realiza la Autoridad de Control al que se refiere el tratamiento, no obstante, si el código se refiere a tratamientos que se realizan en distintos Estados, además de la Autoridad de Control, tendrán que intervenir en la aprobación el Comité, que emitirá su informe sobre si el código presenta o no garantías adecuadas y la Comisión que será el órgano que finalmente lo apruebe. En todo caso la autoridad competente para aprobarlo tendrá que registrarlo y publicarlo mediante cualquier medio apropiado para que está a disposición pública.

Además de la posibilidad de adherirse a códigos de conducta, el Reglamento ofrece a los responsables y encargados la posibilidad de obtener certificados, sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes. La solicitud es voluntaria y el organismo competente para otorgar el certificado o sello será acreditado por la Autoridad de Control. La certificación se expedirá por un período máximo de tres años pudiendo ser renovada en las mismas condiciones, o bien, podrá ser retirada por los organismos de certificación, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para su concesión.

9. Transferencias internacionales

Conforme se señala en el Considerando 101, la transferencia de datos personales a terceros países o a organizaciones internacionales "no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional".

Los supuestos en los que se pueden realizar dichas transferencias vienen recogidos en los arts. 45-49 del Reglamento. En primer lugar, se prevé la existencia de un nivel adecuado de protección respecto del país u organización en cuestión, declarado como tal por la Comisión Europea.

En segundo lugar, si no existe la declaración anterior, se pueden transferir los datos si el país u organización ofrecen garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

En tercer lugar, a falta de los dos requisitos anteriores, se pueden aplicar las excepciones contenidas en el art. 49 que básicamente se refieren a la existencia del consentimiento explicito del interesado, la necesidad de celebrar o ejecutar un contrato entre el interesado y el responsable o en el interés del interesado entre el responsable y un tercero, razones de interés público, la formulación, el ejercicio o la defensa de reclamaciones, la protección de los intereses vitales del interesado o de otras personas, cuando el interesado

esté física o jurídicamente incapacitado para dar su consentimiento. Por último, la excepción que cierra la lista de excepciones del mencionado artículo se refiere a la transferencia realizada desde un registro público que tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta. En este último caso no se podrán transferir la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro.

En cuarto lugar, se podrán transferir datos en base a una decisión del un órgano administrativo o judicial si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

10. Autoridades de control

El art. 51 contiene un mandato para cada uno de los Estados miembros de establecer una o varias autoridades públicas independientes para supervisar la aplicación de lo previsto por el Reglamento. En caso de que haya más de una autoridad, se designará una, que representará a dichas autoridades en el Comité, y se establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia.

El nombramiento de las personas que integren la autoridad de control se debe realizar mediante un procedimiento transparente por el Parlamento, el Gobierno o el Jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

Los titulares de la autoridad de control deben actuar con independencia e integridad, no pueden realizar acciones que sean incompatibles con sus funciones y no pueden participar mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

La competencia de la autoridad de control abarca los tratamientos que se realicen en su territorio, incluidos los realizados por los poderes públicos, pero no aquellos realizados por los tribunales en el ejercicio de su función. En caso de que el tratamiento se realice en más de un Estado miembro, las autoridades tienen la obligación de cooperar y actuar conjuntamente, pero ello no resta que una de ellas deberá actuar como autoridad principal

y el resto como entidades interesadas. Será autoridad principal la del establecimiento principal o del único establecimiento del responsable o del encargado.

Se señala en el Considerando 129 que las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos para garantizar la supervisión y ejecución coherentes del Reglamento en toda la Unión.

Conforme al art. 59, los poderes de las autoridades de control se dividen en poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales.

Por último, señalar que las autoridades de control tienen la obligación de elaborarr un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas que deberán transmitir al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros, así como a la Comisión y al Comité.

11. El Comité europeo de protección de datos

El Comité estará formado por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes y deberá constituirse como organismo independiente de la Unión que tenga personalidad jurídica y actuará con independencia, como órgano de coordinación entre las autoridades de control de los Estados miembros.

El Comité debe contar con una Secretaría, a cargo del Supervisor Europeo de Protección de Datos que deberá seguir exclusivamente las instrucciones del presidente del Comité y responder ante él.

El Comité será el organismo competente para emitir dictámenes en caso de que una autoridad de control lo solicite porque tenga que emitir una decisión que:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos

b) afecte a un asunto cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el Reglamento;

c) tenga por objeto aprobar los criterios aplicables a la acreditación de un organismo, o un organismo de certificación;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros

e) tenga por objeto autorizar las cláusulas contractuales de un contrato entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional

f) tenga por objeto la aprobación de normas corporativas vinculantes de conformidad con el mecanismo de coherencia

Además, el Comité podrá emitir una decisión vinculante cuando:

a) una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad principal, o esta haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) existan puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) una autoridad de control competente no solicite dictamen al Comité en los casos en que este sea obligatorio o, no siga el dictamen del Comité emitido.

Al tratarse de un organismo con personalidad jurídica, sus decisiones podrán ser recurridas ante el TJUE, tanto por las autoridades de control interesadas, como por el responsable, encargados o reclamante.

En conclusión, el Comité ostenta un largo abanico de competencias que se inician bien a través de reclamaciones, o a raíz de las solicitudes de dictámenes y se concretan, conforme se establece en al art. 70 en la promoción de las nuevas figuras recogidas en el Reglamento, asesoramiento, emisión de directrices, control de la implementación, llevanza de un registro público en códigos de conducta y emisión de un informe anual.

12. Recursos, responsabilidad y sanciones

La nueva norma establece que todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y también tiene derecho a la tutela judicial efectiva si considera que se vulneran sus derechos con arreglo al Reglamento o en caso de que la autoridad de

control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger sus datos.

La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

El derecho a la tutela judicial efectiva se ejercitará ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

Además, toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

Por tanto, el Reglamento establece un régimen sancionador en base al cual serán responsables de infracciones de este los responsables y encargados del tratamiento, así como los representantes de los responsables y encargados del tratamiento no establecidos en territorio de la Unión Europea cuando éstos deban ser nombrados a tenor de lo previsto en el art. 27 del Reglamento y también los organismos encargados de la supervisión del cumplimiento de códigos de conducta, y las entidades u organismos de certificación.

Si bien cualquier incumplimiento del Reglamento constituye una infracción, el art. 83 se encarga de tipificar en función de su gravedad, a aquellas que puedan dar lugar a multas administrativas, sin perjuicio de los poderes correctivos de las autoridades de control. Son infracciones muy graves las contenidas en el art. 83.5 y 6 del Reglamento[6] y podrán ser

[6] Art. 83.5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;
b) los derechos de los interesados a tenor de los artículos 12 a 22;
c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;
d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;
e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

sancionadas con multas administrativas de hasta 20.000.000 de euros, como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Las infracciones menos graves están contenidas en el art. 83.4 del Reglamento[7] y podrán ser sancionadas con multas administrativas de hasta 10.000.000 de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Además, conforme al art. 83.7 se habilita a los Estados miembros la posibilidad de establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miemb

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

[7] Art. 83.4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;
b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;
c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.