# Proyecto de exposición de motivos del Consejo: Posición n.º 6/2016 del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo 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)

(2016/C 159/02)

## I. INTRODUCCIÓN

La Comisión propuso el 25 de enero de 2012 una reforma global de la protección de datos, plasmada en:

— la propuesta de Reglamento general de protección de datos de referencia, destinado a sustituir a la Directiva sobre protección de datos de 1995 (antiguo primer pilar);

— una propuesta de Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, destinada a sustituir a la Decisión Marco sobre protección de datos de 2008 (antiguo tercer pilar).

El Parlamento Europeo adoptó su posición en primera lectura sobre la propuesta de Reglamento general de protección de datos el 12 de marzo de 2014 (doc. 7427/14).

El Consejo aprobó una orientación general el 15 de junio de 2015, dando así a la Presidencia un mandato de negociación para entablar diálogos tripartitos con el Parlamento Europeo (doc. 9565/15).

Tanto el Parlamento Europeo (a través de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior) como el Consejo (a través del Comité de Representantes Permanentes) confirmaron, el 17 y el 18 de diciembre de 2015, respectivamente, el acuerdo sobre el texto transaccional que se había negociado durante los diálogos tripartitos.

En su sesión del 12 de febrero de 2016, el Consejo alcanzó un acuerdo político sobre el proyecto de Reglamento (doc. 5455/16). El 8 de abril de 2016, el Consejo adoptó su posición en primera lectura, que concuerda plenamente con el texto transaccional del Reglamento acordado en las negociaciones informales entre el Consejo y el Parlamento Europeo.

El Comité Económico y Social presentó su dictamen sobre el Reglamento en 2012 (DO C 229 de 31.7.2012, p. 90).

El Comité de las Regiones presentó su dictamen sobre el Reglamento en 2012 (DO C 391 de 18.12.2012, p. 127).

El Supervisor Europeo de Protección de Datos fue consultado y emitió un primer dictamen en 2012 (DO C 192 de 30.6.2012, p. 7) y un segundo dictamen en 2015 (DO C 301 de 12.9.2015, pp. 1-8).

La Agencia de los Derechos Fundamentales presentó su dictamen el 1 de octubre de 2012.

## II. OBJETIVOS

El Reglamento general de protección de datos armoniza las normas de protección de datos de la Unión Europea. Los objetivos del Reglamento son reforzar los derechos de las personas en materia de protección de datos, facilitar la libre circulación de datos personales en el mercado único y reducir la carga administrativa.

## III. ANÁLISIS DE LA POSICIÓN DEL CONSEJO EN PRIMERA LECTURA

### A. Observaciones generales

A fin de alcanzar el objetivo del Consejo Europeo de lograr un acuerdo sobre la reforma de la protección de datos a más tardar a finales de 2015, el Parlamento Europeo y el Consejo han celebrado negociaciones informales para hacer converger sus posiciones. El texto de la posición del Consejo en primera lectura sobre el Reglamento general de protección de datos refleja plenamente el acuerdo transaccional alcanzado entre los dos colegisladores, con la asistencia de la Comisión Europea.

La posición del Consejo en primera lectura mantiene los objetivos de la Directiva 95/46/CE, a saber: salvaguardar los derechos en materia de protección de datos y garantizar la libre circulación de datos. Al mismo tiempo, intenta adaptar las normas de protección de datos actualmente vigentes al volumen cada vez mayor de datos personales que son objeto de tratamiento como consecuencia de los cambios tecnológicos y la globalización. A fin de que el Reglamento sea válido en el futuro, las normas sobre protección de datos de la posición del Consejo en primera lectura son neutrales desde el punto de vista tecnológico.

Para garantizar un nivel uniforme de protección de las personas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales en el mercado interior, la posición del Consejo en primera lectura establece en lo esencial un conjunto único de normas que es directamente aplicable en toda la Unión. Esta armonización eliminará la fragmentación derivada de la existencia de diferentes normativas de transposición de la Directiva 95/46 en los Estados miembros. No obstante, a fin de tener en cuenta las exigencias que pueden plantear ciertas situaciones de tratamiento de datos, en particular en el sector público, la posición del Consejo en primera lectura permite a los Estados miembros especificar más pormenorizadamente en su Derecho nacional la aplicación de las normas de protección de datos que se establecen en el Reglamento.

La protección de los datos personales es un derecho fundamental consagrado en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea. Por otra parte, en el artículo 16 del Tratado de Funcionamiento de la Unión Europea se establece que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, cualquiera que sea su nacionalidad o residencia, y que han de establecerse normas a tal efecto y normas sobre la libre circulación de los datos de carácter personal. Sobre esta base, la posición del Consejo en primera lectura establece los principios y normas de protección de las personas físicas por lo que respecta al tratamientos de sus datos personales.

Para lograr los objetivos del Reglamento, la posición del Consejo en primera lectura refuerza la rendición de cuentas de los responsables del tratamiento (responsables de determinar los fines y los medios del tratamiento de datos personales) y de los encargados del tratamiento (responsables de efectuar el tratamiento de los datos personales en nombre del responsable), con el fin de promover una verdadera mentalidad de protección de datos. En este contexto, se ha establecido en todo el Reglamento un planteamiento basado en el riesgo, que permite modular las obligaciones del responsable y del encargado del tratamiento según el riesgo que acarreen las operaciones de tratamiento de datos que llevan a cabo. Los códigos de conducta y los mecanismos de certificación, por su parte, contribuyen al cumplimiento de las normas de protección de datos. Este planteamiento permite evitar el establecimiento de normas excesivamente prescriptivas y reduce las cargas administrativas sin menoscabo del cumplimiento de la normativa. Por otra parte, por su carácter disuasorio, las sanciones que pueden imponerse crean incentivos para que los responsables del tratamiento cumplan el Reglamento.

Las nuevas normas de protección de datos que se establecen en la posición del Consejo en primera lectura refuerzan además los derechos de los ciudadanos y garantizan que sean exigibles. Al lograr así las personas físicas un mayor control sobre sus datos personales, se refuerza la confianza en los servicios en línea a escala transfronteriza, promoviéndose por ende el mercado único digital. Los menores merecen una protección específica, ya que pueden ser menos conscientes tanto de los riesgos que acarrea el tratamiento de datos personales como de sus derechos.

Por lo demás, la posición del Consejo en primera lectura refuerza la independencia de las autoridades de control, armonizando al mismo tiempo sus tareas y competencias. Las normas de cooperación entre las autoridades de control y, cuando ha lugar, entre estas y la Comisión en asuntos transfronterizos -el mecanismo de coherencia- contribuirá a que el Reglamento se aplique de manera uniforme en toda la Unión Europea. Con ello aumentará la seguridad jurídica y se reducirán las cargas administrativas. Por otra parte, gracias al mecanismo de cooperación y coherencia, los responsables y encargados del tratamiento tendrán un interlocutor único con el que abordar las cuestiones relativas a sus operaciones transfronterizas de tratamiento y, en particular, podrán acogerse en caso de conflicto a las decisiones vinculantes que dicte el Comité Europeo de Protección de Datos que se crea a tal efecto. Este mecanismo hará que la aplicación del Reglamento será más coherente. Además, proporcionará más seguridad jurídica y reducirá las cargas administrativas.

Por último, la posición del Consejo en primera lectura establece un marco general para las transferencias de datos personales desde la Unión Europea a destinatarios establecidos en terceros países o a organizaciones internacionales, introduciendo nuevos instrumentos con respecto a la Directiva 95/46/CE.

## B. **Aspectos principales**

El Consejo y el Parlamento Europeo, con la asistencia de la Comisión Europea, han logrado mediante negociaciones informales aproximar las posiciones que habían establecido, respectivamente, en la orientación general del Consejo y en la posición en primera lectura del Parlamento. La posición del Consejo en primera lectura sobre el Reglamento general de protección de datos refleja plenamente el acuerdo transaccional alcanzado. A continuación se exponen los aspectos principales de la posición del Consejo en primera lectura.

1. ***Ámbito de aplicación***

1.1. **Ámbito de aplicación material del Reglamento y articulación con la Directiva sobre protección de datos**

Según la posición del Consejo en primera lectura, el Reglamento general de protección de datos se aplica al tratamiento total o parcialmente automatizado de datos personales y al tratamiento no automatizado de datos personales que formen parte de cualquier conjunto estructurado de datos personales al que se pueda acceder con arreglo a unos criterios determinados, o que estén destinados a formar parte de un conjunto estructurado de esas características. El ámbito de aplicación material del Reglamento general de protección de datos y el ámbito de aplicación de la Directiva sobre protección de datos en el ámbito penal son mutuamente excluyentes. En el Reglamento se precisa que este no se aplica al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, con inclusión de la protección y la prevención frente a las amenazas para la seguridad pública. Esta delimitación permite a las autoridades de las fuerzas y cuerpos de seguridad, en particular a la policía, aplicar, como norma, el régimen de protección de datos de la Directiva, garantizando al mismo tiempo a las personas físicas que son objeto de un proceso penal un nivel elevado y uniforme de protección de los datos personales.

1.2. **Instituciones y órganos de la UE**

Para garantizar una protección uniforme y coherente de los titulares de los datos («los interesados») por lo que respecta al tratamiento de sus datos personales, se indica en la posición del Consejo en primera lectura que, tras la adopción del Reglamento general de protección de datos, se deben efectuar las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, que se aplica a las instituciones, órganos y organismos de la UE, para que ambos Reglamentos sean aplicables al mismo tiempo.

1.3. **Exención de las actividades de tratamiento de carácter doméstico**

A fin de evitar establecer normas que creen cargas innecesarias para los particulares, la posición del Consejo en primera lectura dispone que el Reglamento no se aplicará al tratamiento de datos personales efectuado por una persona física en el ejercicio de una actividad exclusivamente personal o doméstica y, por ende, sin conexión alguna con una actividad profesional o comercial.

1.4. **Ámbito de aplicación territorial**

La posición del Consejo en primera lectura establece condiciones equitativas desde el punto de vista territorial para los responsables y encargados del tratamiento, al incluir en el ámbito de aplicación del Reglamento a todos los responsables y encargados del tratamiento independientemente de que estén o no establecidos en la Unión.

En primer lugar, el Reglamento dispone que todas las normas de protección de datos se aplican al tratamiento de datos personales en el contexto de las actividades de un establecimiento en la Unión del responsable o el encargado del tratamiento, independientemente de que el tratamiento tenga lugar en la Unión o no. En segundo lugar, con el fin de garantizar que las personas físicas no se vean privadas de la protección de sus datos, el Reglamento se aplica al tratamiento de datos personales de los interesados que se encuentren en la Unión, aunque el responsable o el encargado del tratamiento no esté establecido en la Unión, pero siempre que las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, o con la supervisión de sus actos si estos tienen lugar dentro de la Unión Europea. Al determinar el ámbito de aplicación de esta manera, se refuerza, además, la seguridad jurídica de los responsables del tratamiento y de los interesados (es decir, las personas cuyos datos personales son objeto de tratamiento).

La posición del Consejo en primera lectura garantiza también que los interesados y las autoridades de control tengan un punto de contacto en la UE en caso de que los responsables o encargados del tratamiento no estén establecidos en la Unión pero estén incluidos en el ámbito de aplicación del Reglamento, al obligar a estos últimos a designar por escrito un representante en la Unión. Para evitar cargas administrativas innecesarias, esta obligación no se aplica a las operaciones de tratamiento que presenten escasas probabilidades de generar un riesgo para los derechos y libertades de las personas físicas, ni a las operaciones de tratamiento efectuadas por una autoridad u organismo público de un tercer país.

2. ***Principios aplicables al tratamiento de datos personales***

Los principios de la protección de datos se aplican a toda información relativa a una persona física identificada o identificable, incluida la información que ya no pueda atribuirse a una persona concreta sin recurrir a información adicional, siempre que esa información adicional se conserve por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos no se atribuyan a una persona física identificada o identificable (seudonimización). En lo que se refiere a los principios subyacentes al tratamiento de los datos personales, el

Reglamento mantiene en gran medida la continuidad con respecto a la Directiva 95/46/CE. Al mismo tiempo, se ha adaptado el principio de «minimización de datos» para tener en cuenta la realidad digital y para establecer un equilibrio entre, por una parte, la protección de los datos personales y, por otra, las posibilidades de tratamiento de datos de que disponen los responsables del tratamiento.

## 3. *Licitud del tratamiento de datos*

### 3.1. **Condiciones de licitud del tratamiento**

En interés de la seguridad jurídica, la posición del Consejo en primera lectura se basa en la Directiva 95/46/CE para especificar que el tratamiento de datos personales solo será lícito si se cumple al menos una de las siguientes condiciones:

— consentimiento del interesado al tratamiento de sus datos para uno o varios fines específicos;

— existencia de un contrato;

— existencia de una obligación legal;

— necesidad del tratamiento para la protección de los intereses vitales del interesado o de otra persona física;

— necesidad del tratamiento para una misión de interés público o inherente al ejercicio de poderes públicos conferidos al responsable del tratamiento;

— necesidad del tratamiento para intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Dos de estas condiciones merecen un análisis más detenido: el consentimiento y los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

#### 3.1.1. *Consentimiento*

Para permitir que se traten sus datos personales, el interesado puede dar su consentimiento para el tratamiento mediante un acto afirmativo claro que constituya una manifestación de voluntad libre, específica, informada e inequívoca de que acepta el tratamiento de los datos personales que le conciernen. Dicho consentimiento abarca todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Si el tratamiento tiene varios fines, tiene que darse el consentimiento para todos ellos. Además, el responsable del tratamiento debe poder demostrar que el interesado ha dado su consentimiento a la operación de tratamiento. No constituyen consentimiento, por tanto, el silencio, las casillas ya marcadas o la inacción. Esta concepción del consentimiento garantiza la continuidad con el acervo que se ido desarrollando en relación con el uso de este concepto sobre la base de la Directiva 95/46/CE, contribuyendo al mismo tiempo a la interpretación y aplicación comunes del consentimiento en toda la Unión Europea.

Por otra parte, para proteger los derechos del interesado, se especifica que, si este ha dado su consentimiento en el marco de una declaración escrita que también se refiere a otros asuntos, no será vinculante ninguna parte de la declaración que constituya una infracción del Reglamento. Asimismo, al evaluar si el consentimiento se ha dado libremente, debe tenerse en cuenta en sumo grado, entre otras cosas, si la ejecución de un contrato se ha supeditado al consentimiento a operaciones de tratamiento que no son necesarias para la ejecución de dicho contrato.

Por último, con el fin de permitir excepciones a la prohibición general de tratamiento de categorías especiales de datos personales, la posición del Consejo en primera lectura establece para el tratamiento de estos datos condiciones más estrictas que para el resto de los tratamientos: en efecto, el interesado tiene que consentir explícitamente en que se traten ese tipo de datos personales sensibles.

Por lo que respecta a los menores, la posición del Consejo en primera lectura dispone un régimen de protección específico aplicable al consentimiento del menor en relación con la oferta de servicios de la sociedad de la información. El tratamiento de los datos personales de un menor de 16 años es lícito si se puede verificar de una manera razonable, teniendo en cuenta la tecnología disponible, que dicho consentimiento ha sido dado o autorizado por el titular de la patria potestad o tutela sobre el niño. Los Estados miembros pueden establecer una edad menor si lo consideran más adecuado siempre que esta no sea inferior a los 13 años.

3.1.2. *Interés legítimo del responsable del tratamiento*

El tratamiento de datos personales puede ser lícito si es necesario a efectos de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero. No obstante, esos intereses legítimos no bastarán para hacer lícito un tratamiento si sobre ellos prevalecen intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Para determinar si existe un interés legítimo será precisa una evaluación en la que se pondere, entre otras cosas, si el interesado puede prever de forma razonable, en el momento y en el contexto de la recopilación de los datos personales, que pueda producirse el tratamiento con tal fin. El tratamiento de datos personales con fines de mercadotecnia directa puede ser considerado un tratamiento que obedece a un interés legítimo. Dado que corresponde al legislador establecer por ley la base jurídica para que las autoridades públicas traten datos personales, lo anterior no se aplica al tratamiento de datos personales efectuado por las autoridades públicas en el ejercicio de sus funciones.

### 3.2. **Adopción por los Estados miembros de normas específicas de adaptación del Reglamento**

En la posición del Consejo en primera lectura se permite a los Estados miembros mantener o establecer disposiciones más específicas que adapten la aplicación de las normas del Reglamento en caso de que el tratamiento de datos personales se efectúe para cumplir una obligación legal o sea necesario para el desempeño de una función que se lleve a cabo en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Se prevén asimismo excepciones, requisitos específicos y otras medidas en relación con determinadas operaciones de tratamiento, con el fin de que los Estados miembros puedan conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información, el acceso del público a documentos oficiales, el tratamiento del número nacional de identificación, el tratamiento de datos personales en el ámbito laboral y el tratamiento de datos personales con fines de archivo en interés público, con fines de investigación científica e histórica o con fines estadísticos.

### 3.3. **Tratamiento ulterior**

La posición del Consejo en primera lectura dispone que el tratamiento con fines distintos de aquellos para los que hayan sido recogidos inicialmente los datos personales únicamente es lícito si ese tratamiento ulterior es compatible con los fines para los cuales los datos personales se trataron inicialmente. No obstante, si el interesado ha dado su consentimiento o si el tratamiento se atiene a una disposición legislativa de la Unión o del Estado miembro que constituya una medida necesaria y proporcionada en una sociedad democrática para proteger, en particular, objetivos importantes de interés público general, se permite al responsable del tratamiento realizar el tratamiento ulterior, con independencia de la compatibilidad de los fines. Se han reforzado los derechos del interesado en relación con el tratamiento ulterior, en particular en lo que se refiere al derecho a la información y al derecho de oponerse al tratamiento ulterior cuando este no es necesario para el desempeño de una función realizada por razones de interés público.

Con objeto de determinar si el fin al que obedece el tratamiento ulterior es compatible con el fin para el cual se recopilaron inicialmente los datos personales, el responsable del tratamiento debe tener en cuenta, entre otras cosas, toda posible relación entre los fines iniciales y los fines del tratamiento ulterior previsto, el contexto en el que se hayan recopilado los datos personales, en particular las expectativas que razonablemente podía tener el interesado, atendiendo a su relación con el responsable del tratamiento, en cuanto a su utilización ulterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de salvaguardas adecuadas tanto en las operaciones del tratamiento inicial como en las del tratamiento ulterior previsto.

### 3.4. **Tratamiento de categorías especiales de datos personales**

Los datos personales que, por su naturaleza, son especialmente sensibles merecen una protección particular, ya que el contexto de su tratamiento puede generar riesgos importantes para los derechos y libertades fundamentales de las personas. Por esta razón, en la posición del Consejo en primera lectura se mantiene, como norma, el planteamiento de la Directiva 95/46/CE en la prohibición del tratamiento de categorías especiales de datos personales.

Como excepción a esta regla, el tratamiento de datos sensibles se autoriza en ciertos casos que se enumeran taxativamente: por ejemplo, cuando el interesado ha dado su consentimiento explícito, cuando el tratamiento es necesario para atender a un interés público esencial, o cuando el tratamiento es necesario para otros fines relacionados, en particular, con el ámbito de la salud.

Por último, la posición del Consejo en primera lectura faculta a los Estados miembros para establecer condiciones adicionales, incluidas limitaciones, con respecto al tratamiento de datos genéticos, biométricos o relativos a la salud. No obstante, estas otras condiciones no deben constituir un obstáculo para la libre circulación de datos dentro de la Unión.

4. ***Fortalecimiento de la posición del interesado***

4.1. **Introducción**

La posición del Consejo en primera lectura fortalece la posición del interesado al reforzar sus derechos en materia de protección de datos e imponer obligaciones a los responsables del tratamiento. Los derechos del interesado abarcan el derecho de información; el derecho de acceso a los datos personales; el derecho de rectificación o supresión de los datos personales, con inclusión del «derecho al olvido»; el derecho a limitar el tratamiento; el derecho a la portabilidad de los datos; el derecho de oposición; y el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, con inclusión de la elaboración de perfiles. Los derechos que han sufrido cambios importantes con respecto a la Directiva 95/46/CE se precisan a continuación.

Los responsables del tratamiento tienen la obligación de facilitar el ejercicio de los derechos del interesado y de tratar los datos personales respetando el principio de transparencia, en particular facilitando información sobre el tratamiento de datos personales que efectúen.

No obstante, si los datos personales tratados por el responsable del tratamiento no le permiten identificar a una persona física, el responsable del tratamiento no estará obligado a obtener información adicional para identificar al interesado con la única finalidad de dar cumplimiento a una disposición del Reglamento.

A pesar de estos derechos de los interesados y estas obligaciones de los responsables del tratamiento, la posición del Consejo en primera lectura mantiene el planteamiento de la Directiva 95/46/CE al permitir limitaciones de los principios generales y de los derechos de las personas si dichas limitaciones se basan en el Derecho de la Unión o del Estado miembro. Tales limitaciones han de respetar en lo esencial los derechos y libertades fundamentales y ser necesarias y proporcionadas en una sociedad democrática para salvaguardar determinados intereses públicos.

4.2. **Transparencia**

A tenor del principio de transparencia, los responsables del tratamiento deben facilitar la información y las comunicaciones referentes al tratamiento de datos personales en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular en el caso de las informaciones dirigidas a menores. La información debe facilitarse por escrito o por otros medios, si ha lugar por medios electrónicos.

La posición del Consejo en primera lectura establece además los plazos aplicables a las solicitudes de información y a las comunicaciones y demás acciones del responsable del tratamiento, y establece como norma general la gratuidad. No obstante, si las solicitudes del interesado son manifiestamente infundadas o excesivas, especialmente por su carácter repetitivo, el responsable del tratamiento puede cobrar una tasa razonable en función de los costes administrativos soportados para facilitar la información o la comunicación o emprender la acción solicitada, o bien negarse a atender a la solicitud. En estos casos, corresponde al responsable del tratamiento demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

4.3. **Información y comunicaciones que ha de facilitar el responsable del tratamiento**

A fin de encontrar un equilibrio entre la necesidad de facilitar suficiente información al interesado acerca del tratamiento de sus datos personales, por una parte, y, por otra, la necesidad de evitar obligaciones gravosas para el responsable del tratamiento, la posición del Consejo en primera lectura establece un planteamiento en dos etapas para garantizar que se informe adecuadamente a los interesados, tanto en los casos en que los datos personales sean recopilados a partir del propio interesado como cuando dichos datos no se obtengan de él. En la primera etapa, el responsable del tratamiento está obligado a proporcionar al interesado, en el momento en que se obtengan los datos personales, la información que se enumera en el Reglamento. En la segunda, el responsable del tratamiento tiene que facilitar la información adicional que se enumera en el Reglamento y que es necesaria para garantizar un tratamiento lícito y eficiente. Si el responsable del tratamiento tiene intención de proceder a un tratamiento ulterior de los datos personales para un fin distinto de aquel para el cual se recopilaron inicialmente los datos, también debe informar de ello al interesado.

El responsable del tratamiento no estará obligado a facilitar la información mencionada ni en la primera etapa ni en la segunda cuando el interesado ya posea la información. Cuando los datos personales no hayan sido obtenidos del propio interesado, el responsable del tratamiento no dará ninguna información al interesado en caso de que el registro o la comunicación de los datos personales a otras partes estén expresamente establecidos por ley, o cuando facilitar los datos al interesado resulte imposible o exija esfuerzos desproporcionados.

Por último, los responsables estarán obligados a comunicar cualquier rectificación, supresión o limitación del tratamiento a cada uno de los destinatarios a los que el responsable haya revelado datos personales, a menos que resulte imposible o exija esfuerzos desproporcionados. Además, el responsable del tratamiento tiene que informar al interesado acerca de estos destinatarios, si así lo solicita este.

### 4.4. **Iconos**

Los principios de transparencia exigen que el interesado sea informado de la existencia del tratamiento y de sus fines. Teniendo esto en cuenta, la posición del Consejo en primera lectura establece que la información facilitada al interesado puede ir acompañada de iconos formalizados. Los responsables podrán decidir, de manera facultativa, si el uso de dichos iconos formalizados es útil para el tratamiento de los datos que ellos efectúan. Los iconos deberán transmitir de forma visible, inteligible y claramente legible una presentación adecuada del tratamiento de datos previsto. Los iconos se tienen que facilitar de manera simultánea a la información proporcionada. Cuando los iconos se presenten en formato electrónico, tienen que ser legibles por una máquina. Para contribuir al uso formalizado de iconos en la UE, el Reglamento faculta a la Comisión a adoptar actos delegados para especificar qué información debe presentarse por medio de iconos, así como los procedimientos para presentar iconos formalizados. El Consejo Europeo de Protección de Datos tiene que emitir dictamen sobre los iconos propuestos por la Comisión. La posibilidad de adoptar actos delegados no impide que el Consejo Europeo de Protección de Datos emita directrices, dictámenes y mejores prácticas.

### 4.5. **Derecho de acceso**

El titular de los datos tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernan y, en caso de que se confirme el tratamiento, el derecho de acceso a los datos y a la información mencionada en el Reglamento. Teniendo esto en cuenta, el Reglamento especifica que el responsable del tratamiento facilitará gratuitamente una copia de los datos personales sometidos a tratamiento. Por cualquier otra copia solicitada por el interesado el responsable podrá cobrar una tasa razonable basada en los costes administrativos. El derecho mencionado a obtener una copia no deberá afectar negativamente a los derechos y libertades de terceros.

### 4.6. **Derecho a la supresión («derecho al olvido»)**

La posición del Consejo en primera lectura otorga a los interesados el derecho de supresión de los datos personales que les conciernan cuando el tratamiento de tales datos no se ajuste a lo dispuesto en el Reglamento o al Derecho de la Unión o del Estado miembro al que esté sujeto el responsable.

La referencia al «derecho al olvido» reconoce la necesidad de adaptar el derecho de supresión a un contexto digital. Los responsables que hacen públicos datos personales que el interesado desea olvidar tienen que tomar medidas razonables, incluidas las de carácter técnico, para informar a los responsables que estén tratando los datos de la petición del interesado de que se suprima todo enlace a los mismos, o las copias o réplicas de los mismos, teniendo en cuenta la tecnología disponible y el coste de ejecución. El Consejo Europeo de Protección de Datos podrá emitir directrices, recomendaciones y mejores prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de los servicios de comunicación disponibles al público.

El derecho de supresión y la obligación del responsable de informar a los demás responsables de la solicitud de supresión no se aplicará cuando el tratamiento de los datos personales sea necesario para los fines enumerados exhaustivamente en el Reglamento, como la libertad de expresión e información.

### 4.7. **Derecho a la portabilidad de los datos**

La posición del Consejo en primera lectura establece que, cuando el tratamiento de los datos personales se efectúe por medios automatizados, los titulares de los datos tienen derecho a recibir los datos personales que les conciernan, que hayan facilitado a un responsable del tratamiento, en un formato estructurado, de uso habitual, de lectura mecánica e interoperable, y a transmitir estos datos a otro responsable del tratamiento. Además, en la posición se ha precisado que, cuando sea técnicamente posible, el interesado tendrá derecho a que los datos personales se transmitan directamente de un responsable a otro. Con ello se refuerza más el control que los titulares de los datos tienen de sus datos, y se alienta además la competitividad entre los responsables.

No obstante, el derecho a la portabilidad de los datos no se aplica al tratamiento necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento. Por otra parte, cuando un conjunto de datos personales determinado concierna a más de un titular, el derecho del titular a recibir los datos personales se deberá entender sin menoscabo de los derechos y libertades de los otros titulares.

4.8. **Derecho de oposición**

En los casos en que los datos personales puedan ser sometidos a tratamiento legalmente porque el tratamiento sea necesario para el desempeño de un cometido llevado a cabo en interés público o en el ejercicio de una autoridad pública conferida al responsable del tratamiento, o por motivos de los intereses legítimos del responsable del tratamiento o de un tercero, el interesado tendrá derecho a oponerse al tratamiento de cualquier dato personal que concierna a su situación particular. En ese caso, el responsable del tratamiento dejará de poder tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Teniendo esto en cuenta, se especifica que cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tiene derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan. Esto incluye la elaboración de perfiles, en la medida en que dicha elaboración esté relacionada con la mercadotecnia directa. La elaboración de perfiles se define como toda forma de tratamiento automatizado de datos personales consistente en utilizar dichos datos para evaluar determinados aspectos personales propios de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, las preferencias o los intereses personales, la fiabilidad o el comportamiento, la ubicación o los movimientos de dicha persona física. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales no pueden ser tratados para dichos fines. Además, este derecho tendrá que ser indicado de forma explícita y clara al interesado, a más tardar en el momento de la primera comunicación entre el responsable del tratamiento de los datos personales y el interesado.

Por otra parte en la posición del Consejo en primera lectura se incluye una referencia a la característica de no rastreo digital especificando que, en el contexto de la utilización de servicios de la sociedad de la información, el interesado podrá ejercer su derecho a oponerse por medios automatizados recurriendo a especificaciones técnicas.

4.9. **Toma de decisiones individuales automatizadas, incluida la elaboración de perfiles**

Todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que evalúe aspectos personales relativos a él y que produzca efectos jurídicos que le conciernan o que le afecten de modo similarmente significativo. Como, por ejemplo, la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Dicho tratamiento automatizado puede incluir la elaboración de perfiles. No obstante, este derecho a no ser sometido a tratamiento automatizado no se aplicará cuando sea necesario para:

— la celebración o la ejecución de un contrato entre el titular de los datos y un responsable del tratamiento;

— cuando lo autorice el Derecho de la Unión o de un Estado miembro al que el responsable del tratamiento esté sujeto y que establezca igualmente medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como para controlar el fraude o la evasión fiscal; o

— cuando se base en el consentimiento explícito del interesado.

— Excepto en el segundo caso referido al tratamiento autorizado por el Derecho de la Unión o del Estado miembro, el responsable que efectúe el tratamiento por medios automatizados tiene que aplicar medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del titular de los datos. Estas salvaguardas incluirán al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento y la posibilidad de que el interesado exprese su punto de vista e impugne la decisión. Además, para garantizar un tratamiento leal y transparente, el responsable del tratamiento debe utilizar los procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles y medidas que reduzcan al mínimo el riesgo para los intereses del interesado.

Se han otorgado más derechos al titular de los datos, porque se obliga al responsable del tratamiento a facilitar al interesado, cuando sea necesaria para garantizar un tratamiento de datos leal y transparente, información sobre la existencia de un mecanismo de decisión automatizado que comprenda la elaboración de perfiles, y al menos en tales casos información significativa sobre la lógica aplicada, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Por último, la toma de decisiones y la elaboración de perfiles automatizadas basándose en categorías particulares de datos personales solo se permiten en condiciones específicas, que incluyen el derecho del interesado a oponerse a dicho tratamiento cuando estos datos personales se traten con fines de investigación científica e histórica o estadísticos, salvo en caso de que el tratamiento sea necesario para el desempeño de un cometido llevado a cabo en interés público.

El Consejo Europeo de Protección de Datos podrá emitir directrices, recomendaciones y mejores prácticas para precisar más los criterios y condiciones de las decisiones basadas en los perfiles.

## 5. *Responsable del tratamiento y encargado del tratamiento*

### 5.1. **Introducción**

La posición del Consejo en primera lectura establece el marco jurídico en el que se inscribe la responsabilidad del responsable en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. A tenor del principio de rendición de cuentas, el responsable tiene la obligación de aplicar medidas técnicas y organizativas adecuadas y de poder demostrar que sus operaciones de tratamiento se llevan a cabo de conformidad con el Reglamento. Teniendo esto en cuenta, el Reglamento establece normas sobre las responsabilidades del responsable en relación con las evaluaciones de impacto, el mantenimiento de registros de los tratamientos, las violaciones de datos, la designación de un delegado de protección de datos y los códigos de conducta y mecanismos de certificación.

### 5.2. **Evaluaciones de impacto**

Al responsable del tratamiento le corresponde efectuar evaluaciones de impacto de un tratamiento de datos para evaluar si el tratamiento puede acarrear un alto riesgo para los derechos y libertades de las personas. La posición del Consejo en primera lectura establece los casos en los que es necesaria una evaluación de impacto especial de la protección de datos, como determinadas operaciones específicas de tratamiento a gran escala. En caso de que dicha evaluación de impacto indique que las operaciones de tratamiento implican un riesgo elevado que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, tendrá que consultarse a la autoridad de control antes del tratamiento. La autoridad de control podrá, entonces, asesorar al responsable del tratamiento y utilizar cualquiera de sus competencias.

El Consejo Europeo de Protección de Datos puede publicar directrices sobre operaciones de tratamiento que es probable que den lugar a un riesgo elevado para los derechos y libertades de las personas físicas e indicar qué medidas pueden ser suficientes en dichos casos para afrontar un posible riesgo.

### 5.3. **Registros de las actividades del tratamiento**

Para que las autoridades de control puedan efectuar controles a posteriori, el responsable o, en su caso, el representante del responsable, o el encargado del tratamiento tendrá que mantener registros de las actividades de tratamiento que se hayan efectuado bajo su responsabilidad, incluidas las violaciones de datos. Para reducir las cargas administrativas, la obligación de registrar no se aplicará a las empresas u organizaciones que empleen a menos de 250 personas, salvo que el tratamiento que se realice pueda suponer un riesgo para los derechos y libertades de los interesados, no tenga un carácter ocasional o incluya datos sensibles o datos relativos a condenas y delitos penales.

### 5.4. **Violaciones de datos**

Las violaciones de datos personales pueden dar lugar a graves perjuicios físicos, materiales o inmateriales para las personas físicas, entre los que se incluyen la pérdida de control sobre sus datos personales o la restricción de sus derechos, la discriminación, la usurpación de la identidad, las pérdidas financieras, la inversión no autorizada de una seudonimización, el menoscabo de la reputación, la pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social para la persona física en cuestión. La posición del Consejo en primera

lectura dispone que los responsables tienen que notificar las violaciones a las autoridades de control, a menos que sea improbable que la vulneración de los datos personales constituya un riesgo para los derechos y libertades de las personas. Además, deben comunicar a los interesados aquellas violaciones que puedan entrañar un riesgo alto. La notificación a las autoridades de control permitirá a estas intervenir, cuando sea necesario. Además, la comunicación al interesado permitirá a este adoptar medidas cautelares.

Para reducir las cargas administrativas, la posición del Consejo en primera lectura establece umbrales diferentes para las notificaciones a las autoridades de control y las comunicaciones a los interesados, siendo más alto el umbral que se aplica a la comunicación que el de la notificación. Tan pronto como tengan conocimiento de que se ha producido una violación de datos personales, sin demora injustificada y, de ser posible, a más tardar setenta y dos horas después, los responsables tienen la obligación de notificarla a la autoridad de control competente. No obstante, los responsables pueden abstenerse de la notificación si pueden demostrar que es improbable que la violación de datos personales constituya un riesgo para los derechos y libertades de las personas físicas. Aparte de algunas excepciones, los responsables tienen la obligación de comunicar al interesado, sin demora, la violación de los datos, cuando sea probable que dicha violación vaya a dar lugar a un riesgo alto para los derechos y libertades de los interesados.

El Consejo Europeo de Protección de Datos puede formular directrices, recomendaciones y mejores prácticas para definir las violaciones de datos y determinar la demora indebida después de que el responsable haya tenido conocimiento de la violación, y las circunstancias específicas en las que es necesario que el responsable notifique la violación de los datos personales, así como las circunstancias en las que es probable que la violación de los datos constituya un riesgo alto para los derechos y libertades de las personas.

### 5.5. **Delegado de protección de datos**

La finalidad de la designación del delegado de protección de datos es mejorar la observancia del Reglamento. Por eso, el delegado de protección de datos tiene que ser una persona con conocimientos especializados en el Derecho y la práctica relativos a la protección de datos, y tiene que ayudar al responsable o encargado del tratamiento a supervisar la observancia interna del presente Reglamento. Podrá pertenecer a la plantilla del responsable o del encargado del tratamiento o desempeñar las funciones de delegado en el marco de un contrato de servicios. Asimismo podrá designarse a un delegado de protección de datos único para un grupo de empresas, o cuando el responsable o el encargado del tratamiento sea una autoridad pública. La posición del Consejo en primera lectura dispone la designación obligatoria de un delegado de protección de datos cuando:

— el tratamiento lo lleve a cabo una autoridad, a excepción de los tribunales o las autoridades judiciales independientes en el ejercicio de su función jurisdiccional,

— las actividades principales del responsable o encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran un seguimiento periódico y sistemático de los interesados a gran escala; o

— las actividades principales del responsable o encargado del tratamiento consistan en el tratamiento a gran escala de datos sensibles y datos relativos a condenas y delitos penales.

### 5.6. **Códigos de conducta y mecanismos de certificación**

La posición del Consejo en primera lectura incentiva la aplicación de códigos de conducta y promueve un amplio uso de los mecanismos de certificación de la protección de datos y de sellos y marcados de protección de datos. Estas iniciativas contribuyen al respeto de las normas de protección de datos evitando un exceso de normas prescriptivas y reduciendo los gastos para las autoridades públicas responsables de su ejecución. Además, los códigos de conducta pueden tener en cuenta las características específicas del tratamiento efectuado en determinados sectores, así como las necesidades de las microempresas y las pequeñas y medianas empresas. Los mecanismos de certificación y los sellos y marcados de protección de datos, por su parte, contribuyen a la observancia del Reglamento en la medida en que los titulares de los datos pueden evaluar fácilmente el nivel de protección de datos de los productos y servicios correspondientes.

La posición del Consejo en primera lectura comprende un conjunto elaborado de normas en materia de códigos de conducta y mecanismos de certificación, sellos y marcados de protección de datos que dejan espacio para la iniciativa privada, preservando al mismo tiempo las normas de protección de datos gracias a la participación de las autoridades de control.

5.6.1. *Códigos de conducta*

La autoridad de control puede aprobar códigos de conducta y modificaciones o ampliaciones de esos códigos de conducta. Cuando el proyecto de código de conducta guarde relación con actividades de tratamiento en varios Estados miembros, antes de su aprobación la autoridad de control competente tiene que someter el proyecto de código o de modificación o ampliación del mismo al Consejo Europeo de Protección de Datos para que este dictamine.

La Comisión podrá adoptar actos de ejecución para decidir que los nuevos códigos de conducta y las modificaciones o ampliaciones de códigos de conducta existentes aprobados por la autoridad de control competente tengan validez general dentro de la Unión.

El Consejo Europeo de Protección de Datos ha de promover la elaboración de códigos de conducta. También tiene que recopilar en un registro todos los códigos de conducta aprobados y las modificaciones de los mismos, y ponerlos a disposición del público a través de cualquier medio adecuado.

5.6.2. *Mecanismos de certificación, sellos y marcados de protección de datos*

La posición del Consejo en primera lectura establece que cada Estado miembro tiene que disponer si los organismos de certificación son acreditados por la autoridad de control o por el Organismo Nacional de Acreditación. Los organismos de certificación acreditados pueden certificar a los responsables y encargados basándose en los criterios aprobados por la autoridad de control competente o, de conformidad con el mecanismo de coherencia, por el Consejo Europeo de Protección de Datos. En este último caso, los criterios aprobados por el Consejo Europeo de Protección de datos podrán dar lugar a una certificación común: el Sello Europeo de Protección de Datos. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años con posibilidad de renovación. El organismo de certificación tiene que comunicar a la autoridad de control las razones de la concesión de la certificación solicitada o de su retirada. A continuación, la autoridad de control puede rechazar o declarar inválida dicha certificación.

La Comisión estará facultada para adoptar actos delegados a fin de especificar las condiciones que deben tenerse en cuenta en relación con los mecanismos de certificación en materia de protección de datos. El Consejo Europeo de Protección de Datos tiene que emitir dictamen sobre dichas condiciones. La Comisión podrá adoptar también actos de ejecución sobre normas técnicas relativas a los mecanismos de certificación y los sellos y marcados de protección de datos, y modalidades para promover y reconocer los mecanismos de certificación y los sellos y marcados de protección de datos.

Por último, el Consejo Europeo de Protección de Datos debe promover el establecimiento de mecanismos de certificación en materia de protección de datos y sellos y marcados de protección de datos.

## 6. *Transferencia de datos personales a terceros países u organizaciones internacionales*

### 6.1. **Introducción**

Los flujos transfronterizos de datos personales hacia y desde los países no pertenecientes a la Unión y las organizaciones internacionales son fundamentales en el contexto del comercio global y de la economía digital transfronteriza. El nivel de protección que la Unión garantiza no tiene que verse disminuido cuando los datos personales de ciudadanos de la UE se transfieren fuera de la Unión.

Como principio general, solo se puede llevar a cabo una transferencia de datos personales a un tercer país u organización internacional si los responsables y encargados respetan las normas enunciadas en el Reglamento. La posición del Consejo en primera lectura tiene plenamente en cuenta la jurisprudencia del Tribunal de la Unión Europea, incluida su sentencia del 6 de octubre de 2015 en el asunto C-362/14. La posición del Consejo en primera lectura mantiene diferentes vías para permitir las transferencias transfronterizas de datos personales, aunque refuerza las garantías de respeto de los derechos de protección de datos. Estas vías diferentes de transferencia de datos personales son: decisiones de adecuación, garantías adecuadas y excepciones.

La posición del Consejo en primera lectura aclara que cualquier sentencia de un órgano jurisdiccional o resolución de una autoridad administrativa de un tercer país por la que se exija a un responsable o encargado del tratamiento transferir o hacer públicos datos personales únicamente podrá ser reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional entre el país tercero que formula la solicitud y la Unión o un Estado miembro. Asimismo, la posición del Consejo en primera lectura especifica explícitamente que dichos acuerdos internacionales se entienden sin perjuicio de otros motivos para las transferencias transfronterizas previstos en el Reglamento.

6.2. **Decisiones de adecuación**

Una transferencia internacional podrá producirse sobre la base de una decisión de adecuación de la Comisión según la cual un tercer país, o un territorio o uno o varios sectores especificados de ese tercer país, o la organización internacional de que se trate proporcionan un nivel de protección fundamentalmente similar al que se garantiza en la Unión. Así se garantiza en toda la Unión la seguridad y la uniformidad jurídicas.

La Comisión puede decidir revocar una decisión de adecuación, tras haber avisado y presentado una justificación completa al tercer país u organización internacional. La Comisión adopta las decisiones de adecuación y las decisiones de revocación de tales decisiones como actos de ejecución. Los actos de ejecución tienen que disponer un mecanismo de revisión periódica, al menos cada cuatro años. La Comisión debe supervisar las nuevas situaciones que se produzcan en los países terceros y organizaciones internacionales que puedan afectar al funcionamiento de las decisiones de adecuación. A los efectos del seguimiento y la realización de las revisiones periódicas, la Comisión debe tomar en consideración los puntos de vista y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. En el contexto de la evaluación y revisión del Reglamento, la Comisión tiene que informar regularmente al Consejo y al Parlamento Europeo. Por último, el Consejo Europeo de Protección de Datos tiene que emitir un dictamen destinado a la Comisión sobre la adecuación del nivel de protección en un tercer país o una organización internacional, en particular para evaluar si han dejado de garantizar un nivel de protección suficiente.

Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas por una Decisión de la Comisión. Del mismo modo, las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE y las decisiones adoptadas por la Comisión de conformidad con el artículo 64, apartado 4, de la Directiva 95/46/CE siguen siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control o por decisión de la Comisión, respectivamente. Al garantizar la continuidad, la posición del Consejo en primera lectura proporciona seguridad jurídica.

6.3. **Garantías adecuadas**

Además de mediante decisiones de adecuación, las transferencias transfronterizas pueden producirse también cuando el responsable o el encargado del tratamiento adoptan garantías para compensar la falta de protección de los datos en el tercer país u organización internacional. Tales garantías pueden consistir en hacer uso de normas corporativas vinculantes, cláusulas tipo de protección de datos adoptadas por la Comisión, cláusulas tipo de protección de datos adoptadas por una autoridad de control o cláusulas contractuales autorizadas por una autoridad de control. Los responsables o encargados del tratamiento en terceros países podrán también proporcionar garantías adecuadas para las transferencias de datos personales a terceros países u organizaciones internacionales. Pueden hacerlo mediante un código de conducta aprobado, junto con unos compromisos vinculantes y de obligado cumplimiento de aplicar las garantías adecuadas a través de instrumentos contractuales u otros jurídicamente vinculantes, en particular en lo que se refiere a los derechos de los interesados. Pueden hacerlo también mediante un mecanismo de certificación aprobado por la autoridad de control competente junto con unos compromisos vinculantes y de obligado cumplimiento del responsable o el encargado del tratamiento en el tercer país de aplicar las garantías adecuadas, incluso en lo que se refiere a los derechos de los interesados.

6.4. **Excepciones**

A falta de una decisión de adecuación o de garantías adecuadas, una transferencia o conjunto de transferencias de datos personales a un tercer país o una organización internacional podrá producirse sobre la base de las excepciones que se numeran exhaustivamente en el Reglamento. Una de esas excepciones se refiere a los intereses legítimos perseguidos por el responsable en caso de que los intereses o los derechos y libertades del interesado no queden anulados por dichos intereses. A fin de contar con garantías suficientes para las transferencias transfronterizas de datos personales, los intereses legítimos del responsable están regulados estrictamente y solo podrán invocarse como solución de última instancia. Para garantizar una aplicación coherente del Reglamento, el Consejo Europeo de Protección de Datos tiene que elaborar, a iniciativa propia o a instancia de la Comisión, directrices, recomendaciones y mejores prácticas para precisar más los criterios y requisitos de las transferencias de datos cuando no exista una decisión de adecuación o las garantías adecuadas.

7. ***Autoridades de control***

7.1. **Independencia**

Con el fin de proteger los derechos y las libertades fundamentales de las personas en lo que respecta al tratamiento de sus datos personales y de facilitar la libre circulación de datos personales en la Unión, cada Estado miembro dispondrá que una o varias autoridades públicas independientes se encarguen de supervisar la aplicación del presente Reglamento. Cada autoridad de control y sus miembros actuarán con total independencia, y también con integridad, en el cumplimiento de los cometidos que le hayan sido encomendados y en el ejercicio de los poderes que hayan sido conferidos a dicha autoridad de control ya sus miembros.

Cada autoridad de control tiene que contribuir a la aplicación coherente del presente Reglamento en toda la Unión. A este efecto, las autoridades de control tienen que cooperar entre sí y con el Consejo Europeo de Protección de Datos, así como con la Comisión. Para lograr una aplicación coherente del Reglamento es necesario establecer en el Reglamento las competencias de las autoridades de control y definir los cometidos y los poderes de investigación, poderes correctivos y poderes de autorización y consultivos que las autoridades de control deben poseer, como mínimo.

### 7.2. **Secreto profesional**

La posición del Consejo en primera lectura establece normas sobre el secreto profesional para las autoridades de control y sus miembros. En primer lugar, el o los miembros y el personal de cada autoridad de control tienen que estar sujetos, conforme al Derecho de la Unión o del Estado miembro, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus cometidos o en el ejercicio de sus poderes. Se ha precisado además que, durante su mandato, este deber de secreto profesional se aplica en particular a la información a particulares de infracciones al Reglamento. Por otra parte, al Consejo Europeo de Protección de Datos le corresponde emitir directrices, recomendaciones y mejores prácticas para establecer procedimientos comunes para informar a las personas de las infracciones al Reglamento.

## 8. *Cooperación y coherencia*

### 8.1. **Comité Europeo de Protección de Datos**

En la posición del Consejo en primera lectura, el Comité Europeo de Protección de Datos queda constituido como órgano de la Unión con personalidad jurídica para garantizar una aplicación correcta y coherente del Reglamento. Las intervenciones del Comité consisten en concreto en emitir dictámenes, adoptar decisiones vinculantes en el contexto de la resolución de litigios entre autoridades de control y formular directrices sobre cualquier cuestión relativa a la aplicación del presente Reglamento, con el fin de garantizar la aplicación coherente del mismo.

El Comité Europeo de Protección de Datos está compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos. La Comisión puede participar en las actividades y reuniones del Comité Europeo de Protección de Datos, sin derecho a voto. Los debates del Comité Europeo de Protección de Datos son confidenciales cuando el mismo lo considere necesario, tal como prevé su reglamento interno.

Cuando el Comité Europeo de Protección de Datos adopte una decisión vinculante en el contexto de la resolución de un litigio, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones que se refieran a los principios y normas aplicables a las instituciones, órganos, oficinas y agencias de la Unión que correspondan en cuanto al fondo a los contempladas en el Reglamento.

### 8.2. **Mecanismo de coherencia**

En los casos de tratamiento transfronterizo de datos personales en los que esté involucrada más de una autoridad de control, el mecanismo de coherencia garantiza que se adopte una decisión única, la cual será aplicable en toda la Unión Europea, aunque se tendrá en cuenta la opinión de las diferentes autoridades de control afectadas. Por consiguiente, el mecanismo de coherencia aumenta la proximidad entre los interesados y la autoridad de control que toma las decisiones, implicando a las autoridades «locales» de control en la toma de decisiones. Además, en caso de litigio entre autoridades de control de los diferentes Estados miembros, el recién creado Comité Europeo de Protección de Datos es competente para adoptar decisiones vinculantes.

Las normas del mecanismo de coherencia no se aplicarán cuando el tratamiento sea efectuado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente es la autoridad de control del Estado miembro en el que la autoridad pública o el organismo privado esté establecido.

La posición del Consejo en primera lectura prevé que se examinen la cooperación y el mecanismo de coherencia cuando la Comisión efectúe una evaluación del Reglamento.

## 9. *Recursos, responsabilidad y sanciones*

La posición del Consejo en primera lectura establece un conjunto detallado de normas que permite a los interesados varias vías de recurso judicial, en particular la reclamación de una indemnización en caso de perjuicios como consecuencia de una infracción del Reglamento.

9.1. **Derecho a presentar una reclamación y derecho a la tutela judicial**

La posición del Consejo en primera lectura dispone que todo interesado tiene derecho a presentar una reclamación ante una autoridad de control, si considera que el tratamiento de sus datos personales no se ajusta a lo dispuesto en el presente Reglamento. Todo interesado tiene, además, derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le afecte. Asimismo tiene derecho a la tutela judicial efectiva en caso de que la autoridad de control no dé curso a la reclamación o no informe sobre el curso o sobre el resultado de la misma.

Cada interesado tiene derecho, además, a la tutela judicial efectiva cuando considere que los derechos que le asisten en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales no conforme al presente Reglamento.

La proximidad entre el interesado y el órgano jurisdiccional nacional queda garantizada por el derecho del interesado a obtener la revisión de la decisión de autoridad de protección de datos por su órgano jurisdiccional nacional, sea cual sea el Estado miembro en el que esté establecido el responsable o encargado del tratamiento. Las acciones contra un responsable o encargado del tratamiento tienen que ejercerse ante los órganos jurisdiccionales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los órganos jurisdiccionales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de su poder público.

Por último, toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia de la Unión Europea recurso de anulación de decisiones del Consejo Europeo de Protección de Datos, en las condiciones previstas en el artículo 263 del TFUE.

9.2. **Representación de los interesados**

El interesado tiene el derecho de dar un mandato a órganos, organizaciones o asociaciones que cumplan determinados criterios específicos, como trabajar sin ánimo de lucro y realizar actividades en el ámbito de la protección de datos, para presentar una reclamación en su nombre y ejercitar los derechos a un recurso judicial efectivo en su nombre y el derecho a recibir una indemnización en su nombre, cuando así lo disponga el Derecho del Estado miembro. Estos criterios específicos pretenden evitar el desarrollo de hábitos de reclamación comercial en el ámbito de la protección de datos. Por otra parte, los Estados miembros pueden disponer que cualquier entidad, organización o asociación de ese tipo tenga, con independencia del mandato del interesado, derecho a presentar en dicho Estado miembro una reclamación ante la autoridad de control competente y a ejercer los derechos a un recurso judicial, si considera que se han vulnerado los derechos del interesado a consecuencia de un tratamiento de datos personales que no se ajusta al Reglamento.

9.3. **Suspensión de los procedimientos**

Para evitar que el mismo asunto referente al tratamiento por parte del mismo responsable o encargado sea examinado por diferentes órganos jurisdiccionales, cualquier órgano jurisdiccional competente distinto de aquel ante el cual se interpuso la demanda en primer lugar puede suspender los procedimientos o, a instancia de una de las partes, inhibirse.

9.4. **Derecho a indemnización y responsabilidad**

La posición del Consejo en primera lectura dispone que todo interesado que haya sufrido un perjuicio material o inmaterial como consecuencia de una vulneración del Reglamento tiene derecho a recibir del responsable o el encargado del tratamiento una indemnización. Para dar la posibilidad a los interesados de reclamar una indemnización en caso de sufrir perjuicios, y al mismo tiempo proporcionar seguridad jurídica a los responsables y encargados del tratamiento, el Reglamento especifica sus responsabilidades. Cualquier responsable que participe en el tratamiento es responsable de los daños causados. El encargado del tratamiento es responsable solo cuando no haya cumplido las obligaciones del Reglamento que atañen específicamente a los encargados del tratamiento, o haya actuado al margen o en contra de las instrucciones legales del responsable. No obstante, un responsable o encargado del tratamiento estará exento de responsabilidades si consigue probar que no es en modo alguno responsable del hecho que haya dado lugar al perjuicio.

Cuando más de un responsable o encargado, o un responsable y un encargado hayan participado en el mismo tratamiento y sean responsables de cualquier perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de la totalidad del perjuicio, a fin de garantizar la indemnización efectiva al interesado. No obstante, cuando un responsable o encargado haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en ese mismo tratamiento la parte de la indemnización que corresponda a su parte de responsabilidad por el perjuicio ocasionado.

9.5. **Sanciones**

Con objeto de garantizar el cumplimiento del Reglamento, la posición del Consejo en primera lectura dispone que las autoridades de control puedan imponer multas administrativas. Estas multas deberán ser efectivas, proporcionadas y disuasorias. Los Estados miembros podrán establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro. Aparte de la imposición de multas administrativas, las autoridades de control también pueden hacer uso de poderes correctivos, como dictar advertencias o apercibimientos. Para aumentar la armonización, el Comité Europeo de Protección de Datos tiene que elaborar unas directrices destinadas a las autoridades de control sobre la aplicación de los poderes correctivos de la autoridad de control y la fijación de las multas administrativas.

La posición del Consejo en primera lectura contiene una lista de criterios a partir de los cuales la autoridad de control decidirá si impone una multa administrativa y, en caso afirmativo, de qué cuantía. Estos criterios se refieren, entre otras cosas, a la naturaleza, gravedad y duración o a la intencionalidad o negligencia de la infracción al Reglamento. En el Reglamento se enumeran tanto las infracciones como las multas administrativas máximas correspondientes. Dentro de los márgenes de estas multas administrativas máximas, la autoridad de control ha de determinar la cuantía apropiada en función de las circunstancias de cada infracción particular. Para proporcionar seguridad jurídica a los responsables y encargados del tratamiento y aumentar la armonización de las multas administrativas en la Unión al tiempo que se reserva un margen de discreción para las autoridades de control, estas infracciones se subdividen en tres categorías. Las infracciones de la primera categoría relativas a las obligaciones de los responsables y encargados pueden ser sancionadas con un máximo de 10 000 000 euros o, tratándose de una empresa, con el 2% como máximo del total del volumen de negocios anual mundial del ejercicio financiero anterior, si este importe es superior. La segunda categoría de infracciones a los derechos de los interesados y a los principios generales con un máximo de 20 000 000 euros o el 4% del volumen de negocios. La tercera categoría de infracciones relativas al incumplimiento con una resolución de la autoridad de control y también una multa máxima de 20 000 000 euros o el 4% del volumen de negocios.

10. ***Situaciones específicas de tratamiento de datos***

10.1. **Tratamiento de datos personales y libertad de expresión y de información**

Los Estados miembros deben disponer por ley la conciliación del derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información, incluido el tratamiento de datos personales para fines periodísticos y fines de expresión académica, artística o literaria. Para garantizar la transparencia por lo que respecta a la conciliación de estos derechos, los Estados miembros tienen la obligación de notificar a la Comisión las disposiciones correspondientes de su legislación y las modificaciones de dichas disposiciones, así como las nuevas disposiciones pertinentes.

10.2. **Tratamiento en el ámbito laboral**

Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral.

Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad de los interesados, así como sus intereses legítimos y sus derechos fundamentales. Los Estados miembros tienen que notificar a la Comisión las disposiciones correspondientes de su legislación y las modificaciones de dichas disposiciones, así como las nuevas disposiciones pertinentes.

10.3. **Garantías y excepciones aplicables al tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**

La posición del Consejo en primera lectura establece normas específicas para el tratamiento de datos personales con fines de archivo en interés público, con fines de investigación científica e histórica o con fines estadísticos. Estas normas tienen como finalidad conciliar, por una parte, el interés de disponer de datos para alimentar los archivos, facilitar estadísticas y realizar investigaciones y, por otra, los derechos de protección de datos.

El tratamiento de datos personales con fines de archivo en interés público, con fines de investigación científica e histórica o con fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el Reglamento. Se autoriza a los Estados miembros a facilitar, en condiciones concretas y con las garantías adecuadas para los interesados, especificaciones y excepciones a los requisitos de información y a

los derechos a la rectificación, a la supresión, al olvido, a la limitación del tratamiento y a la portabilidad de los datos, así como al derecho de oposición cuando se traten datos personales con fines de archivo en interés público, con fines de investigación científica e histórica o con fines estadísticos.

La posición del Consejo en primera lectura también permite excepciones a la prohibición de tratar datos personales sensibles en caso de tratamiento de datos personales con fines de archivo en interés público, con fines de investigación científica e histórica o con fines estadísticos. Dicha excepción se permite si el tratamiento en cuestión se basa en el Derecho de la Unión o de los Estados miembros: dicho tratamiento tiene que ser proporcional al objetivo perseguido, respetar la esencia del derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

11. ***Acuerdos celebrados anteriormente***

La posición del Consejo en primera lectura precisa que los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes de la entrada en vigor del presente Reglamento y que se ajusten a lo dispuesto en la legislación de la Unión aplicable antes de la entrada en vigor del presente Reglamento seguirán en vigor hasta que sean modificados, sustituidos o revocados. Con ello se garantiza seguridad jurídica a los responsables y se evitan cargas administrativas innecesarias a los Estados miembros. Además, hay que en cuenta que para modificar los acuerdos vigentes los Estados miembros dependen de la cooperación de los terceros países u organizaciones internacionales.

IV. **CONCLUSIÓN**

La posición del Consejo en primera lectura refleja el acuerdo transaccional alcanzado, con ayuda de la Comisión, en las negociaciones entre el Consejo y el Parlamento Europeo. El Consejo insta al Parlamento Europeo a aprobar formalmente la posición común en primera lectura sin enmiendas, con el fin de que pueda crearse el nuevo marco legislativo de la UE para la protección de los datos, la cual reforzará los derechos de protección de datos facilitando al mismo tiempo que facilita el flujo de datos personales en el mercado digital.