

I

El Anteproyecto de Ley modifica el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, para transponer la Directiva (UE) 2021/2118 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2021, por la que se modifica la Directiva 2009/103/CE relativa al seguro de la responsabilidad civil que resulta de la circulación de vehículos automóviles, así como al control de la obligación de asegurar esta responsabilidad. Asimismo, incorpora las modificaciones propuestas en el Informe Razonado publicado por la Comisión de Seguimiento del Sistema de Valoración para mejorar el marco legal de la cuantificación de las indemnizaciones por daños corporales en accidentes de circulación.

Se trata, en definitiva, y desde la perspectiva del Derecho a la Protección de datos personales, de una norma que tiene por objeto la mejora de la gestión régimen del aseguramiento obligatorio de vehículos a motor en diferentes aspectos, incluyendo una revisión del sistema de valoración de las lesiones de las víctimas de los accidentes de tráfico, o una ampliación del sistema de cobertura mediante la nominación del Consorcio de compensación de seguros (CCS), o de OFESAUTO como organismo encargado, en determinados casos y circunstancias, -junto a la subsistente, general, de las entidades aseguradoras, de abonar indemnizaciones derivadas de daños, personales o materiales, consecuencia de accidentes de vehículos a motor. Nos encontramos pues, con datos personales de los interesados (en este caso, las víctimas de los accidentes), cuyas lesiones, secuelas o daños y perjuicios en general, van a ser objeto de tratamientos de datos por estas entidades para llegar, en última instancia, al abono de dichos daños o perjuicios, bien mediante tratamientos médicos bien mediante resarcimiento en forma de capital o renta, etc. según las modalidades y circunstancias del caso.

Se trata por tanto de tratamientos de datos realizados por una variedad de responsables o encargados del tratamiento: por las aseguradoras, por el CCS, por OFESAUTO, por peritos médicos, por los Institutos de Medicina Legal y Ciencias Forenses, etc., que pueden incluso entrañar transferencias internacionales de datos, a países incluso fuera de la UE o del Espacio Económico Europeo (EEE). En todos estos casos, es posible, y frecuentemente se tratarán, datos de salud. El RGPD define, art. 4.15), «datos relativos a la

salud» como datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

El concepto de “dato relativo a la salud” del art. 4.15) RGPD es un concepto autónomo de derecho europeo que ha de ser objeto de interpretación uniforme en toda la UE.

Tal y como expresa el TJUE (véanse apartados 81 y ss. de la STJUE de 22 de junio de 2021, C-439/19),

*81 A este respecto, procede recordar que el tenor de una disposición de Derecho de la Unión que no contenga una remisión expresa al Derecho de los Estados miembros para determinar su sentido y su alcance debe normalmente ser objeto de una interpretación autónoma y uniforme en toda la Unión (sentencias de 19 de septiembre de 2000, Linster, C-287/98, EU:C:2000:468, apartado 43, y de 1 de octubre de 2019, Planet49, C-673/17, EU:C:2019:801, apartado 47).*

El RGPD no contiene ninguna remisión al derecho nacional acerca del concepto de “datos relativos a la salud”, por lo que el alcance de este habrá de ser objeto de interpretación uniforme en el seno de la UE. Por ello, la interpretación acerca del concepto y el alcance de “datos relativos a la salud” no puede ser diferente en un Estado miembro que en otro.

De manera algo más extensa, el Considerando (35) establece:

Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Acoge pues, el RGPD, un concepto amplio de “dato relativo a la salud”, incluyendo el “riesgo” de padecer enfermedades (futuras), y, por lo tanto, aunque no exista tal enfermedad hoy, o ni siquiera llegue a materializarse

efectivamente ese “riesgo” (sujeto, como tal riesgo de salud, a una probabilidad) en el futuro.

El RGPD, por otro lado, señala, en su Considerando (51), que los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, [...] el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Es decir, el RGPD, como antes el Convenio 108, o la Directiva 95/46, reconoce que, si bien todos los datos personales afectan al interesado, existen algunos datos que son particularmente sensibles, y le afectan incluso en grado superior. Como ha establecido el Tribunal Constitucional, en Sentencia 76/2019, de 22 de mayo de 2019, respecto de las categorías especiales de datos, también llamados datos sensibles, *el uso de estos (...) es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad*.

El TJUE, desde la sentencia Lindqvist, de 6 de noviembre de 2003, C-101/01, ha acogido un concepto amplio de “dato sensible” o de “datos de categorías especiales”, lo que reitera en sus más recientes sentencias, de las que cabe destacar, por ejemplo, la sentencia de 1 de agosto de 2022, Gran Sala, C-184/20, OT, que en estos particulares establece:

125 Además, una **interpretación amplia** de los conceptos de «categorías especiales de datos personales» y de «datos sensibles» se ve **respaldada** por el objetivo de la Directiva 95/46 y del RGPD, a que se ha hecho mención en el apartado 61 de la presente sentencia, de asegurar un alto nivel de protección de las libertades y de los derechos fundamentales de las personas físicas, en particular, de su intimidad, en relación con el tratamiento de los datos personales que las afectan (véase, en este sentido, la sentencia de 6 de noviembre de 2003, Lindqvist, C-101/01, EU:C:2003:596, apartado 50).

126 Más aún, la interpretación contraria se opondría a la finalidad del artículo 8, apartado 1, de la Directiva 95/46 y del artículo 9, apartado 1, del RGPD, que consiste en garantizar una mayor protección frente a tales tratamientos, que, en atención a la particular sensibilidad de los datos objeto de ellos, pueden constituir, como se desprende del considerando 33 de la Directiva 95/46 y del considerando 51 del RGPD, una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, garantizados por los artículos 7 y 8 de la Carta [véase, en este sentido, la sentencia de 24 de septiembre de 2019, GC y otros (Retirada de enlaces a datos sensibles), C-136/17, EU:C:2019:773, apartado 44].

En consecuencia, ha de interpretarse el concepto de “dato sensible” de una manera amplia.

Pues bien, a pesar de la importancia para los interesados y los riesgos que conlleva el tratamiento de datos de salud para el derecho fundamental a la protección de datos, no existe en la MAIN un Análisis de Riesgos, y como consecuencia de dicho Análisis, una Evaluación de Impacto en Protección de Datos (EIPD) de la que puedan resultar los riesgos y medidas que puedan mitigar estos, para que los tratamientos de datos personales que resultan de la norma no interfieran más allá de lo estrictamente necesario en el derecho fundamental a la protección de datos de que disfrutaban las personas físicas.

Esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos puedan tener como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma (ley, real decreto etc.) quien realice una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto “Otros impactos”, el análisis del “impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma”.

*g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma*

Dicho análisis de riesgos o la EIPD no se ha llevado a cabo por el órgano proponente del proyecto.

Esta Agencia recuerda, asimismo, que el reiterado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de

Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta “los riesgos que se derivan del tratamiento de los datos personales” (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), en su caso, lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el proyecto de Real Decreto establece (ver art. 35.7.d) RGPD). Al no haber una EIPD no se conocen cuáles son esos riesgos que derivan de los tratamientos de datos personales que establece la norma, por lo que a esta Agencia no se le han ofrecido ni los riesgos ni en consecuencia las posibles medidas y garantías que paliarían esos riesgos

Corresponde, cabe recordar, al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, y que ello habrá de hacerlo “desde el diseño” del tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento, y ello aconsejaría que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el análisis de riesgos, se incorporen a la propia norma.

Por otra parte, el artículo 35.3 RGPD establece que la EIPD se requerirá en particular en el caso de: a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o la c) observación sistemática a gran escala de una zona de acceso público.

En el presente caso, en que la norma regula tratamientos masivos de datos de salud (categorías especiales de datos), cabe entender que se produce el caso b) anterior, que se plasma en la Lista publicada por la AEPD “LISTAS DE TIPOS DE TRATAMIENTOS DE DATOS QUE REQUIEREN EVALUACIÓN

DE IMPACTO RELATIVA A PROTECCIÓN DE DATOS (art 35.4)”, en su apartado 4: *“Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos”.*

No existe, en definitiva, en el Proyecto o en la MAIN, un análisis del impacto en materia de protección de datos del que resulte los riesgos para este derecho o las medidas propuestas en la norma para mitigar estos.

Pero tampoco se establece en la norma cuál es la base jurídica que legitima, de entre las contempladas en el art. 6.1 RGPD, los distintos tratamientos que contempla, o cuál es la causa que levanta la prohibición del tratamiento de los datos de salud que establece el art. 9.1 RGPD.

Respecto del art. 6.1 RGPD, en los epígrafes c) y e), para los tratamientos necesarios para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; o cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, el art. 6.3 requiere que dichos tratamientos han de venir establecidos por el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La LOPDGDD, a su vez, requiere que dichos tratamientos solo podrán considerarse fundados en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, y respecto de las categorías especiales de datos (entre ellos, datos de salud) el art. 9.2 establece que

*2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.*

*En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.*

Luego la propia LOPDGDD ya contempla la posibilidad de que los datos de salud puedan ser objeto de tratamiento, entre otros supuestos, cuando sea



necesario para la ejecución de un contrato de seguro del que el afectado sea parte.

Ahora bien, el proyecto no hace mención alguna a las características de los tratamientos, bases legitimadoras, medidas adecuadas para mitigar los riesgos derivados de los tratamientos de datos de salud, etc.

Cabe aquí recordar que el art. 9.1 RGPD prohíbe el tratamiento de datos relativos a la vida sexual o la orientación sexual de una persona física. Esta prohibición no será de aplicación cuando concurra alguna de las circunstancias del art. 9.2, circunstancias que corresponde al prelegislador determinar, de manera expresa, en la norma, para que la base legitimadora del tratamiento sea conocida de los interesados.

No se desprende, por tanto, de la norma, si los tratamientos de los datos de salud que contemplan se basan en la letra g) del art. 9.2, o en la letra h) o i), siendo así que los requisitos para la validez de estos son diferentes, ni cuáles son las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado contempladas en la norma.

## II

La sentencia del Tribunal Constitucional (STC) 76/2019, de 22 de mayo, contiene la doctrina relevante sobre el derecho fundamental a la protección de datos personales, y aborda tanto las características como el contenido que ha de tener la normativa que pretenda establecer una injerencia en ese derecho fundamental.

*(...) Por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (artículo 81.1 CE), ora limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). (...) Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, **esa norma legal** «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «**ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención**» (STC 49/1999, FJ 4). En otras palabras, «**no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites**» (STC 292/2000, FJ 15).*

Y ello porque, en el ámbito de las categorías especiales de datos personales, (...) el Reglamento general de protección de datos

*establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, **no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales**, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, **tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles**, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden ser, muy diversos entre sí. El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que el Derecho del Estado miembro establezca **«medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»** [artículo 9.2.g) RGPD] y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.*

En consecuencia, y tal y como exige el Tribunal Constitucional, la norma que establezca unas determinadas injerencias en el derecho fundamental a la protección de datos personales de los interesados de categorías sensibles requiere que dicha norma, en primer lugar, sea una norma con rango de ley, y que, además:

a) especifique el interés público esencial o la causa que justifica el levantamiento de la prohibición de tratamiento que fundamenta la restricción del derecho fundamental (FJ 7 de la STC 76/2019). La ley habrá de explicitar de manera expresa cuál es la causa de entre las previstas en el art. 9.2 RGPD que fundamenta la injerencia al derecho fundamental a la protección de datos personales y ello, el Tribunal Constitucional, con cita de su STC 292/2000, rechaza que dicha identificación de los fines legítimos de la restricción pueda realizarse mediante conceptos genéricos o fórmulas vagas.

b) en segundo lugar, dicha ley habrá de regular pormenorizadamente las injerencias al derecho fundamental estableciendo reglas claras sobre el alcance y contenido de los tratamientos de datos que autoriza. Es decir, habrá de establecer cuáles son los presupuestos y las condiciones del tratamiento de datos personales relativos a las categorías especiales de datos personales que



pueden incluirse en dichos registros mediante reglas claras y precisas (STC 76/2019, FJ 7 b)

c) Y, por último, la propia ley habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El TC ha sido claro en cuanto a que:

*[l]a previsión de las garantías adecuadas **no puede deferirse a un momento posterior a la regulación legal** del tratamiento de datos personales de que se trate. **Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento**, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...)*

Tampoco sirve que para el establecimiento de dichas garantías adecuadas y específicas se pretenda remitirse al propio RGPD o a la LOPDGDD.

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, y el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

La STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:

*En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C 311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

*65 Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C 311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).*

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: *Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].*

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos.

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

*176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].*

### III

Esta AEPD considera, por tanto, que sería muy conveniente que el proyecto de ley contuviera un análisis de los riesgos y la evaluación de los impactos de estos (EIPD) en los tratamientos de datos personales, que permitiera no sólo determinar en la norma las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado, sino establecer del mismo modo las circunstancias esenciales que permiten un tratamiento lícito de dichos datos personales, como recuerdan y requieren las sentencias del TC y del TJUE a que se ha hecho referencia en el epígrafe anterior. Dicho análisis, evaluación de impacto y establecimiento en la norma de las circunstancias que permiten y las medidas adecuadas y específicas que legitiman la incidencia en el derecho fundamental a la protección de datos personales debería de llevarse a cabo con la ayuda del Delegado de Protección de datos correspondiente.

Por otra parte, esta AEPD es consciente del proyecto de ley presentado a informe es transponer la Directiva 2021/2018. Sin embargo, como se ha mencionado al principio y resulta de la propia exposición de motivos y de la MAIN, su propósito es más amplio, porque incorpora las modificaciones propuestas en el Informe Razonado publicado por la Comisión de Seguimiento del Sistema de Valoración para mejorar el marco legal de la cuantificación de las indemnizaciones por daños corporales en accidentes de circulación, que, en definitiva, supone una modificación del sistema de baremo en el ámbito limitado en que dicho informe actúa. Ahora bien, el Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor no contiene una regulación general sobre la protección de datos personales en los tratamientos que se derivan de dicha norma, y sólo en el art. 25, al referirse a la obtención de información del Consorcio de Compensación de Seguros, dice que la Dirección General de Tráfico o la entidad aseguradora proporcionará estos datos al Consorcio de Compensación de Seguros, *y se establecerán*, en todo caso, las medidas técnicas y organizativas necesarias para asegurar la confidencialidad, seguridad e integridad de los datos y las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Se refiere por tanto a un aspecto específico de los tratamientos, pero refiriéndose a una norma hoy derogada, y sin que dichas medidas, para otros tratamientos se recojan en la ley. Y en cualquier caso no se propone la modificación de este art. 25.

Esta AEPD considera que debería de producirse una actualización de la norma conforme al RGPD, ya que esta no se ha producido con la entrada en vigor del RGPD ni de la LOPDGDD, de manea que se lleve a cabo una regulación completa de los tratamientos de datos regidos por esta ley.

Desde un punto de vista práctico, esta Agencia ha publicado recientemente (abril 2023) su **Guía** denominada **“Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo”** <sup>1</sup>, que tienen como objeto servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de la Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas legislativas de las Administraciones Públicas implican el tratamiento de datos personales. Este documento está orientado a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el RGPD, así como la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (L.O. 7/2021). Asimismo, está dirigido a los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir al desempeño de sus funciones de asesoramiento en relación con dichos proyectos normativos.

En esta “Guía” se contienen, con profundidad y rigor, los pasos o el método a seguir para determinar la necesidad y el contenido de la Evaluación de Impacto, y entre ellos esta AEPD desea resaltar en este momento el apartado D del epígrafe II del mismo, relativo a las características de la norma que ampara el tratamiento:

***Toda medida legislativa que habilite un tratamiento debe cumplir con la premisa de “previsto en la ley”. Esto implica que debe ser clara y precisa, y su aplicación accesible y previsible para sus destinatarios, de conformidad con el TEDH, el TJUE y el Tribunal Constitucional (TC). Por lo tanto, en la norma han de estar claramente definidos, con precisión y apropiadamente:***

*1.- La finalidad o finalidades del tratamiento.*

*2.- La legitimidad del tratamiento.*

*3.- La descripción de la implementación del tratamiento en sus aspectos relevantes, como pueden las operaciones y los procedimientos determinantes del tratamiento (por ejemplo, recogida, almacenamiento, acceso, transmisión, difusión,...), las tecnologías planteadas para implementar las operaciones (inteligencia artificial, almacenamiento en Nube, biometría, IoT, móviles, videovigilancia,...), la existencia de*

<sup>1</sup> <https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>

*decisiones automatizadas, así como la participación o posible participación de encargados y/o subencargados en distintas operaciones del tratamiento, entre otros.*

*4.- El ámbito y extensión del tratamiento con relación a las categorías de datos personales tratados (especialmente si son categorías especiales), las categorías de interesados afectados, las circunstancias en las que se utiliza la información personal (por ejemplo: de forma sistemática, solo en determinados casos, durante un periodo de tiempo limitado, etc.), los plazos de conservación de los datos, la frecuencia de recogida de datos, la granularidad de los datos y otros factores que definan el alcance del tratamiento.*

*5.- Los responsables/corresponsables o categorías de responsables y, en su caso, los encargados o categorías de encargos y/o de subencargados.*

*6.- Las entidades que acceden y a las que se pueden comunicar datos personales, así como los fines de tal comunicación, en particular, **las condiciones de la comunicación de datos entre autoridades públicas en virtud de una obligación legal para el ejercicio de una misión oficial** según las condiciones del RGPD (Cons. 31):*

- **En el marco de una investigación concreta.***
- **De interés general.***
- **De conformidad con el Derecho de la Unión o de los Estados miembros.***
- **Por escrito y de forma motivada.***
- **Con carácter ocasional.***
- **No deben referirse a la totalidad de un fichero.***
- **No deben dar lugar a la interconexión de varios ficheros.***

*7.- La justificación de la solución adoptada para el acceso a datos personales, teniendo en cuenta que supone la utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos.*

*8.- Las **medidas para garantizar un tratamiento lícito y equitativo, habida cuenta de la naturaleza, alcance (especialmente con relación a las categorías especiales de datos), contexto y finalidades del tratamiento** o de las categorías de tratamientos, los mecanismos de información y transparencia, así como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX del RGPD, en particular, aquellas orientadas a evitar los accesos o las transferencias de datos ilícitos o abusivos.*

*9.- En el caso de limitación por ley de derechos u obligaciones al amparo de los arts. 23 del RGPD o 24 de la L.O. 7/2021, debe estar muy clara su determinación, las condiciones específicas de limitación de las obligaciones y derechos (Cons. 19 del RGPD), y los perjuicios concretos a la consecución de los fines que justifican la falta de información a los interesados sobre la limitación. La lista anterior no es exhaustiva, sino que cualquier otra disposición pertinente, para cada caso concreto, debería incluirse en la descripción del tratamiento.*

En cuanto a las características esenciales de los tratamientos que la norma habría de recoger (y a las que ya se ha hecho referencia en el párrafo inmediato anterior), esta Agencia sugiere que el Proyecto que ahora se informa recoja, en esta materia, los preceptos, adaptándolos a su caso, que ya se han aprobado en leyes como las siguientes:

- Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte, ver Disposición Adicional (DA) cuarta;
- Ley 20/2022, de 19 de octubre, de Memoria Democrática, DA décima;
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, Título VI, arts. 30 y 32.
- Ley 3/2023, de 28 de febrero, de Empleo, art. 16.
- Ley 7/2023, de 28 de marzo, de protección de los derechos y el bienestar de los animales, art. 10, apartados 2, 4, 5, 6, 7, y art. 12.

#### IV

Respecto a las cuestiones específicas que resultan del articulado del proyecto sometido a informe:

1. Se modifica el art. 2, apartado 2 del Real Decreto Legislativo 8/2004 (en adelante RDLeg 8/2004) para añadir dos párrafos, del siguiente tenor:

*La información a la que se refiere el párrafo anterior será objeto de tratamiento automatizado por el Consorcio de Compensación de Seguros y estará disponible para su consulta a través de su sitio web, de acuerdo con lo que se determine reglamentariamente. El Consorcio de Compensación de Seguros establecerá las medidas adecuadas para*



*facilitar el acceso a la información con inmediatez. Reglamentariamente se determinarán los casos en los que la información deba referirse exclusivamente a si un vehículo está o no asegurado en determinado momento y aquellos otros en los que, además, proceda informar de la entidad aseguradora y del historial de aseguramiento del vehículo.*

*El Consorcio de Compensación de Seguros y el Ministerio de Interior, a través de la Dirección General de Tráfico, coordinarán sus actuaciones para el adecuado ejercicio de sus respectivas competencias en este ámbito, y podrán acceder con tal fin a los datos que figuren en sus ficheros correspondientes.*

La consulta por cualquier tercero de los datos personales que puedan contenerse en el sitio web del CCS constituye un tratamiento de datos personales regido por el RGPD y la LOPDGD, y los criterios para su consulta, en cuanto que suponen una injerencia en el derecho fundamental a la protección de datos, deberían de establecerse en una norma con rango de ley, como se ha expuesto con anterioridad en este Informe.

El segundo párrafo establece un acceso de los datos que para los fines propios de cada una de ellas tiene el CCS y la DGT. Debe aquí recordarse, como se recoge en nuestra Guía ya tan citada, la doctrina del Tribunal Constitucional contraria a los tratamientos masivos de datos personales, recogida en su sentencia 17/2013, de 31 de enero de 2013, conforme a la cual (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley.

En consecuencia, el acceso recíproco a los datos de cada uno de dichos organismos habrá de cumplir con dichas condiciones, lo que sería conveniente que se recogiera en la norma.

2. Se da nueva redacción al art. 2.4 del RDLeg 8/2004. El segundo y tercer párrafo de este precepto se refieren a los tratamientos de datos personales cuando sea necesario a efectos de combatir la conducción de vehículos sin seguro en España. Ahora bien, estos párrafos se limitan a reproducir, en esencia, el art. 4.2 de la Directiva 2009/103, en la redacción dada por la Directiva 2021/2118. Y, sin embargo, dicho art. 4.2 de la Directiva requiere otra cosa, puesto que impone al Derecho del Estado Miembro (en este caso España, y su RDLeg. 4/2008) el establecimiento de las medidas adecuadas para preservar los derechos y libertades y los intereses legítimos del interesado, sin que de la Directiva resulte que se pueden diferir el

establecimiento de esas medidas a “las autoridades” (esto es, a los responsables de los tratamientos) regulados en dicho precepto.

Así, el art. 4.2 de la Directiva establece:

***Sobre la base del Derecho del Estado miembro al que esté sujeto el responsable del control, podrá procederse al tratamiento de datos personales cuando sea necesario a efectos de combatir la conducción de vehículos sin seguro en Estados miembros que no sean aquel en cuyo territorio tengan su estacionamiento habitual. Dicho Derecho deberá ser conforme con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y establecer también medidas adecuadas para preservar los derechos y libertades y los intereses legítimos del interesado.***

*En particular, esas medidas de los Estados miembros especificarán la finalidad exacta del tratamiento de datos, se remitirán a la correspondiente base jurídica, cumplirán los requisitos pertinentes de seguridad, respetarán los principios de necesidad, proporcionalidad y limitación de la finalidad, y fijarán un período de conservación de datos proporcionado.*

Por lo tanto, esta AEPD considera que dichas medidas *deben* establecerse, como requiere la Directiva, en la norma de derecho nacional que permite los tratamientos de datos para dichas finalidades, sin que sea suficiente la mera remisión a “las autoridades” responsables de los tratamientos.

3. El párrafo siguiente del art. 2.4 del RDLeg 8/2004 regula los períodos de conservación de dicha información, y su texto ha de ser modificado para recoger el texto de la Directiva con exactitud para incluir la palabra “inmediatamente” en el lugar adecuado, pues el texto del RDLeg no es totalmente consecuente con ella, y puede dar lugar a interpretaciones que difieran de la Directiva. Así, esta frase en este párrafo debería de redactarse de la siguiente manera:

*(...) Cuando un control del seguro muestre que un vehículo está cubierto por el seguro obligatorio en virtud del artículo 3, el responsable del control suprimirá **inmediatamente** dichos datos. (...)*

4. En el art. 7.1 se pasa de una redacción:

*La información de interés contenida en los atestados e informes de las Fuerzas y Cuerpos de Seguridad encargadas de la vigilancia del tráfico que recojan las circunstancias del accidente podrá ser facilitada por éstas a petición de las partes afectadas, perjudicados o entidades*

*aseguradoras, salvo en el caso en que las diligencias se hayan entregado a la autoridad judicial competente para conocer los hechos, en cuyo caso deberán solicitar dicha información a ésta.*

A esta redacción:

*Las Fuerzas y Cuerpos de Seguridad encargadas de la vigilancia del tráfico facilitarán de forma gratuita a petición de los perjudicados, entidades aseguradoras, o sus representantes, y del Consorcio de Compensación de Seguros copia del atestado o informe equivalente en el que conste toda la información sobre las circunstancias del accidente, salvo en el supuesto de que los hayan entregado a la autoridad judicial competente, en cuyo caso deberán solicitar dicha información a ésta.*

Como explicación, la MAIN (p. 20) recoge que ello se realiza como respuesta a la necesidad de regular el acceso a los atestados y garantizar que se obtengan con la mayor rapidez, calidad, y en todos los casos donde existan lesiones, aunque se trate de lesiones leves. Tanto las entidades aseguradoras como el Consorcio de Compensación de Seguros han resaltado la importancia del atestado, como medio para conocer las circunstancias del accidente, los grados de responsabilidad y las consecuencias dañosas.

Se establece pues una obligación de entrega del atestado, que recoge datos personales sensibles (datos de salud, lesiones, posibles delitos por conducción temeraria o bajo los efectos de sustancias etc.) a terceros distintos del interesado (titular de los datos personales) sin haberse realizado un análisis de los riesgos que ello supone para el derecho fundamental de las personas implicadas, especialmente para el lesionado, y se impone, sin que la ley establezca medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado (véanse art. 9.2.g) RGPD).

Este tratamiento de datos personales incumbe muy principalmente a datos de salud, y el proyecto no recoge, específicamente, cual es la base jurídica que concede licitud a dicho tratamiento (art. 6 RGPD) ni tampoco cuál de las circunstancias del art. 9.2 RGPD levantan la prohibición de tratamiento de dichos datos establecida en el art. 9.1.

Esta AEPD no entra aquí, ciertamente, en si esta medida es o no positiva para los consumidores (véase MAIN, p. 113), y probablemente lo sea porque agiliza, según declara la MAIN, la gestión de los accidentes, pero ello no justifica que la norma non recoja sobre qué se realiza dicho tratamiento, o qué causa levanta la prohibición de tratamiento de dichos datos, que supone entregar a terceros datos personales de salud del perjudicado.

Cabe de nuevo reiterar aquí la doctrina del Tribunal Constitucional, en su sentencia 76/2019, de 22 de mayo, citada extensamente en el epígrafe II de este Informe, y la del TJUE, según la cual la ley que regule el tratamiento habrá

de regular pormenorizadamente las injerencias al derecho fundamental estableciendo reglas claras sobre el alcance y contenido de los tratamientos de datos que autoriza. Es decir, habrá de establecer cuáles son los presupuestos y las condiciones del tratamiento de datos personales relativos a las categorías especiales de datos personales que pueden incluirse en dichos registros mediante reglas claras y precisas (STC 76/2019, FJ 7 b). Y, por último, la propia ley habrá de contener las garantías adecuadas (...).

5. En el art. 11, apartado 1, del RDLeg 8/2004 se recoge que:

*(...) Sin perjuicio de la indemnización que le corresponda abonar con arreglo a lo señalado en los párrafos anteriores y del ejercicio de su derecho de recobro de los importes indemnizados, el Consorcio de Compensación de Seguros remitirá a la autoridad competente en materia sancionadora en la forma que reglamentariamente se determine los datos y documentos que resulten necesarios de entre los que hubieran fundamentado la gestión de la indemnización a los efectos del ejercicio por dicha autoridad de sus potestades sancionadoras.*

Nos encontramos aquí con que unos datos personales, obtenidos por el CCS para el ejercicio de sus competencias como órgano de información o de indemnización, van a ser “tratados” para una finalidad diferente de aquella para la que se recogieron inicialmente los datos personales. Esta nueva finalidad, que se basa en el precepto de la ley que lo recoge, requiere, como establece el art. 6.4 RGPD, que dicho nuevo tratamiento, diferente del inicial, “constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1 RGPD (...)”.

A este respecto, nada en la norma establece para cuál de esos objetivos que se indican en el art. 23.1 RGPD constituye este nuevo tratamiento “una medida necesaria y proporcional en una sociedad democrática” para salvaguardar dichos objetivos. Esta circunstancia es, como se ha venido recogiendo en este Informe, consecuencia de la falta de un análisis integral, desde el punto de vista del derecho fundamental a la protección de datos personales, de los tratamientos de datos que resultan de la norma, de sus bases jurídicas, de las medidas adecuadas y necesarias para salvaguardar el derecho de los interesados etc. que aquí se pone de nuevo de manifiesto.

Por lo demás, en este apartado concreto, no se sabe cuáles son esas “autoridades sancionadoras” a la que se refiere, pudiendo ser cualquiera, pues la norma no restringe ninguna, de las más variadas (autoridades de tráfico, por el accidente; de armas, si hubiere armas implicadas; sanitarias, si hubiere medicamentos en el accidente; de transportes, si se hubiera producido el accidente con daños para los bienes públicos, etc.). En definitiva, esta norma no se considera, en su actual redacción, conforme al RGPD, pues no permite determinar cuáles son los posibles tratamientos a que se refiere.

Del mismo modo, existe indeterminación en cuanto a los datos que el CCS puede “remitir a la autoridad competente”, pudiendo, según dicha redacción, incluir “los datos y documentos que resulten necesarios de entre los que hubieran fundamentado la gestión de la indemnización”, sin limitación alguna y sin referirse a base jurídica alguna que justifique dicha cesión (vid art. 6.4 RGPD ya citado), pudiendo entenderse incluido en dicha redacción incluso datos de salud, lo que no se considerar tampoco conforme al RGPD, por cuanto tampoco se menciona causa alguna del art. 9.2 RGPD que levante la prohibición del tratamiento de dichos datos del art. 9.1 RGPD. Y lo mismo cabe decir de que dicha cesión (tratamiento) se permita “en la forma que reglamentariamente se determine”, como ya hemos puesto de manifiesto, y por las mismas razones en cuanto a que es la ley la que ha de establecer las condiciones de los tratamientos.

6. En ese mismo artículo 11.1 se recoge, en varios apartados, que el Consorcio de Compensación de Seguros podrá celebrar acuerdos con los organismos de otros Estados miembros para cooperar en el intercambio de información y en la gestión de las indemnizaciones en los casos de insolvencia de aseguradoras de vehículos automóviles. La misma referencia se hace sobre OFESAUTO en el art. 27. Con carácter general cabe decir que en estos casos la transferencia de datos que se realicen a un tercer país está sujeta, en todo caso, a los requisitos del Capítulo V del RGPD (arts. 44 y ss.), y quizás sea conveniente que se establezcan en la ley los supuestos en que dichas transferencias a Estados no miembros de la UE pueden tener lugar y sobre qué bases de las previstas en los arts. 44 y ss. RGPD.

7. Por último, esta AEPD desea hacer constar, tras la revisión de los comentarios en la fase de audiencia pública al texto del proyecto, y que se han aportado con la MAIN, que se ha puesto de manifiesto en algún caso una preocupación, que esta Agencia comparte plenamente, acerca de cómo se comunican, por qué vías, la información que resulta del accidente -que puede incluir incluye datos sensibles, de salud- a las compañías aseguradoras (lo que sería extensible al CCS y a OFESAUTO) para la gestión de los expedientes que han de dar lugar a la indemnización del daño al perjudicado. La comunicación de esos datos ha de hacerse de manera que quede asegurada “desde el diseño” la confidencialidad y seguridad de los mismos, y corresponde al responsable del tratamiento (en este caso, las compañías aseguradoras) el establecimiento de un sistema que proteja los datos “desde el diseño” (art. 25 RGPD) y que tenga las condiciones de “seguridad” que establece el art. 32 RGPD, y en particular que garantice confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. No se trata, por tanto, sólo, de que se puedan remitir los datos de salud a la aseguradora mediante un sistema rápido y eficaz, sino que dicho sistema debería de ser obligatorio, establecido en la ley, y que la ley asegurase que dicho sistema habrá de cumplir los requisitos de seguridad del art. 32 RGPD, desde el diseño. La falta de dicho sistema en los responsables es considerada

una infracción, prevista en el art. 83.4.a) RGPD. Se considera conveniente que en la ley se recoja esta obligación de las compañías aseguradoras de contar con un sistema que permita a los perjudicados comunicarse con ellas y enviar documentación de forma segura.