

**014/2024**

1. Con fecha 27 de abril de 2023, la AEPD emitió informe 37/2023 en relación con el Anteproyecto de Ley (APL) por la que se 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. En el mismo (página 12), se observó que debería de producirse en dicho texto legal una actualización de la norma conforme al RGPD (ya que mencionaba a la LOPD1999 etc.), de manera que se lleve a cabo una regulación completa de los tratamientos de datos conforme al RGPD y la LOPDGDD, y además recomendaba que se incorporase a la MAIN el análisis de riesgos y la EIPD.

2. Con la finalidad de recoger las sugerencias de la AEPD, por el Ministerio proponente se incluyó en el APL tras el informe de la AEPD un nuevo Título V para incluir la normativa relativa a la protección de datos de carácter personal. En el capítulo I del Título V del nuevo APL se regulan las disposiciones generales y, dentro de estas, la normativa aplicable, el tratamiento de datos personales en el marco de la celebración del contrato de seguro, el tratamiento de los datos personales durante la vigencia del seguro y para la valoración, gestión y tramitación de siniestros, y el tratamiento de datos de salud en caso de siniestro. En el capítulo II se regulan los sistemas comunes de información para el cumplimiento de lo establecido en el artículo 2.7, los sistemas comunes de información para la prevención del fraude en el seguro y las disposiciones comunes a los sistemas comunes de información.

3. El proyecto se remitió al Consejo de Estado. El Consejo de Estado, mediante escrito de 18 de marzo de 2024, devolvió el expediente al Ministerio de Economía por dos motivos. Uno es que no se había remitido un segundo informe de la AEPD informando sobre el (nuevo) Título V, y otro que el Consejo de Estado advierte que en la MAIN no incorpora consideración alguna sobre el análisis de riesgo y la Evaluación de Impacto en materia de protección de datos (EIPD). El Consejo de Estado refiere que un informe explicativo de la Dirección General de Seguros (DGS) se limita a señalar que se ha realizado, y los factores que han tenido en consideración. El Consejo de Estado añade en su escrito que el referido Título V no figuraba en la versión del APL que se sometió a audiencia e información pública. A tal fin, señala que considera necesario que se recabe el informe de la AEPD para que pueda emitir su parecer respecto del nuevo Título V, y que se complete la MAIN en relación con el análisis de riesgos y la EIPD.

4. Posteriormente (25 de marzo) se plantea a la AEPD petición de informe sobre el referido nuevo Título V de la ley, y entre los documentos figura una denominada EIPD de fecha 22 de marzo de 2024.

## I

En relación con el Título V del Texto Refundido (TR) incluido en el anteproyecto (arts. 144 a 150 del TR), esta AEPD muestra su opinión positiva, en general, y sin perjuicio de algún comentario que se realizará a continuación, al contenido del Título V mencionado pues el mismo recoge, con afán de generalidad y exhaustividad, la regulación de los tratamientos de datos que se llevan a cabo en el ámbito de las actividades de tratamiento en la materia del seguro obligatorio de responsabilidad civil por la circulación de vehículos, y con una sistemática apropiada, ya que distingue entre tratamientos de datos personales destinados a la celebración del contrato de seguro obligatorio y tratamientos durante la vigencia del seguro, con un precepto destinado expresamente al tratamiento de los datos de salud en caso de siniestro. El capítulo II se dedica a los tratamientos de datos personales en el ámbito de los sistemas comunes de información regulados inicialmente en el art. 99.7 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

1. El art. 145.1 señala como base legitimadora del tratamiento para los tratamientos de datos personales de los “interesados que hubiesen solicitado la contratación del seguro” que se lleven a cabo para la celebración del contrato de seguro, así como para la consulta de los sistemas comunes de información dirigidas a dicha finalidad, el art. 6.1.b) RGPD, esto es, cuando “el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales”, lo que se considera correcto.

2. El segundo párrafo del apartado 2 del art. 145 establece que “con la misma finalidad” podrán recabarse y tratarse “información de terceros”, si se cuenta con base jurídica para ello. En principio sería correcto, pero el principio de minimización de datos requeriría que se explicitase cuáles son esos terceros cuyos datos podrían tratarse a los efectos de la celebración de un contrato en el que no son parte. Ciertamente podría citarse aquí al conductor habitual o al asegurado si son distintos del tomador -que sería quien ha “solicitado” el seguro y que se regula en el párrafo inmediato anterior-, pero convendría que la ley restringiera expresamente cuáles son esos terceros a los que se refiere.

3. En el apartado 1 del art. 146 esta AEPD sugiere que cuáles sean las actividades comprendidas en la expresión “las restantes finalidades establecidas en la normativa del seguro *privado*” (sic) se expliciten en la ley o

se suprima, por indeterminada, puesto que cabe considerar que la expresión utilizada en dicho apartado *“para las finalidades relacionadas con su adecuado mantenimiento, desarrollo, gestión y revisión (...) o respecto de las que dispongan de una base jurídica que las legitime de conformidad con lo establecido en la normativa de protección de datos personales”*, ya cubre las finalidades posibles de los tratamientos de datos, sin que se corra el riesgo, por mantener la expresión mencionada, de que se puedan llevar a cabo tratamientos de datos personales que no resulten de una normativa con rango de ley. Y ello además porque, como ya se explicita en este mismo precepto 146.1, para cualesquiera otras finalidades los tratamientos de datos habrán de contar con su correspondiente base jurídica (lo que incluye a la propia ley, vid art. 6.1.c) RGPD), por lo que esta expresión nada añade, es redundante y confusa.

4. El art. 147 del anteproyecto regula los tratamientos de los datos de salud en caso de siniestro. En concreto, como circunstancia que levanta la prohibición de tratamiento establecida en el art. 9.1 RGPD el APL establece el art. 9.2.f) RGPD, esto es, por considerar dicho tratamiento necesario para la formulación, el ejercicio o la defensa de reclamaciones. Sin embargo, esta AEPD considera que esa circunstancia no se dará en todo caso, esto es, no necesariamente siempre deberá de haber una “reclamación”, en el sentido del RGPD, y aun así la aseguradora deberá tratar los datos de los perjudicados para el cumplimiento de las obligaciones derivadas del contrato de seguro (o directamente de la ley cuando exista responsabilidad incluso sin seguro -ex art. 11 por ejemplo-). El precepto señala como causa “la acción directa” de la que dispone el perjudicado en virtud del art. 7.1. El Considerando (52) in fine RGPD parece considerar que el concepto de “reclamación” que justifica el tratamiento de datos sensibles en este caso requiere de “ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial”. Sin necesidad en este momento de debatir sobre esta cuestión, es lo cierto que esta AEPD considera que los tratamientos de datos personales de salud en el ámbito del seguro pueden venir amparados en otra circunstancia distinta del art. 9.2 RGPD, aun cuando no exista “reclamación” en el sentido del art. 9.2.f) RGPD (con independencia de cuál sea la amplitud de este término). El Considerando (54) RGPD señala:

*(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) nº 1338/2008 del Parlamento Europeo y del Consejo ( 1 ), es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades*

*de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este **tratamiento de datos relativos a la salud por razones de interés público** no debe dar lugar a que terceros, como empresarios, **compañías de seguros** o entidades bancarias, traten los datos personales con otros fines.*

Esto es, el art. 9.2.g) RGPD establece como circunstancia que levanta la prohibición del art. 9.1 el “interés público esencial”, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. No parece que quepa discusión acerca de que la “salud pública”, tal y como la describe precisamente el citado Considerando es, por tanto, un interés público esencial. Así lo ha considerado, en cualquier caso, el legislador español, en la Disposición adicional decimoséptima, (DA 17ª) Tratamientos de datos de salud, en su apartado 1, de la LOPDGDD:

*1. Se encuentran amparados en las **letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud** y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:*

*a) (...)*

*h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.*

Del mismo modo, el art. 9.2, segundo inciso, de la LOPDGDD considera amparados los tratamientos de datos de salud en los arts. 9.2 g), h) e i) RGPD, entre otros casos, en concreto cuando así lo exija la ejecución de un contrato de seguro del que el afectado sea parte. La expresión “en particular” que utiliza al comienzo de dicho precepto implica que dichos supuestos contemplados no son exhaustivos, sino ejemplificativos, esto es, no son los únicos tratamientos de datos de salud que puedan considerarse incluidos en el art. 9.2.g) RGPD, como por otra parte se comprueba en la ya citada DA 17ª LOPDGDD, puesto que la propia ley 20/2015 incluye tratamientos de datos de salud en los que no el perjudicado no es el tomador del seguro, y dichos tratamientos habrán de considerarse amparados bajo el art. 9.2.g) RGPD.

En definitiva, en este punto, esta AEPD considera que el tratamiento de los datos de salud en caso de siniestro no estaría amparado únicamente por el art. 9.2.f) RGPD, sino que, bien al contrario, esa circunstancia del apartado f) adicional (y contingente, esto es, podrá darse o no) a la establecida en el art. 9.2.g) RGPD, “interés público esencial”, en relación con el Considerando (54) RGPD y art. 9.2 y DA 17ª de la ley 20/2015. Esta AEPD sugiere que se dé una

nueva redacción al art. 147 del APL que recogiese esta circunstancia como la principal que ampara el tratamiento de los datos de salud en caso de siniestro. Cabe añadir, además, que esta consideración haría innecesaria una justificación como la que se contiene en la redacción del art. 147 para la causa justificativa del art. 9.2.f): la referencia a la acción directa que tiene el perjudicado, y ello porque el RGPD no requiere, en su art. 9.2.f), que los tratamientos amparados en esta circunstancia se lleven a cabo “sobre la base del Derecho de la Unión o de los Estados miembros”, como sí se requiere en las letras g), h), i) y j) del art. 9.2. Es decir, la aseguradora, en caso de “reclamación” en el sentido del art. 9.2.f), no necesita, para tratar datos de salud, que la ley nacional o el Derecho de la UE establezca la posibilidad de dicho tratamiento de datos de salud, posibilidad esta que deriva directamente del propio art. 9.2.f). Por otra parte, no cabe olvidar que el tratamiento de dichos datos de salud en virtud del art. 9.2.g) RGPD está limitado, como cualquier otro, por los principios generales del art. 5 RGPD, y en concreto por el principio de minimización de datos, de manera que los datos a tratar serán sólo los adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (art. 5.1.bc) RGPD).

Ello conlleva que, en opinión de esta Agencia, deba suprimirse el párrafo tercero del art. 147.1 del APL, que establece que a los efectos previstos en el artículo 9.2, párrafo segundo, de la LOPDGDD, se considerará que, en virtud de la mencionada acción directa y de lo previsto en el artículo 99.1 de la Ley 20/2015, de 14 de julio, la posición del perjudicado respecto de la aseguradora es asimilable a la de quienes fueran parte en el contrato de seguro. Y ello porque el perjudicado no es objetivamente asimilable al tomador o al asegurado, ya que no es parte del contrato de seguro; por otra parte, como ya hemos expuesto, el art. 9.2, último inciso, LOPDGDD no contiene una lista exhaustiva de tratamientos, y por último porque de mantenerse se incurriría en la incongruencia de que el art. 147.1, en su redacción presentada a informe, toma en consideración como circunstancia que levanta la prohibición del art. 9.2.f) RGPD, pero hace referencia, en el párrafo citado, al art. 9.2 LOPDGDD, que a su vez se remite al art. 9.2.g) RGPD (no al 9.2.f) RGPD).

Por lo tanto, se sugiere que el art. 147 (tanto en el apartado 1 como en el 2) tome como circunstancia que levanta la prohibición de tratamientos de datos de salud, además de citarse, en su caso, el art. 9.1.f) RGPD, el interés público esencial en materia de salud (art. 9.2.g) RGPD y DA 17ª LOPDGDD), lo cual requiere, de todos modos, que la redacción de la ley habrá de ser conforme al art. 9.2.g) RGPD, esto es, que la propia ley deberá establecer “medidas adecuadas y *específicas* para proteger los intereses y derechos fundamentales del interesado”, y no dejarlas al arbitrio de los responsables del tratamiento. Un ejemplo de medida “específica”, y no meramente genérica o potestativa, se observa en el art. 148.3, como es la exigencia de un factor reforzado de verificación y la existencia de un dato personal de identificación del solicitante.



5. En el art. 149.2, primer párrafo, al referirse a los datos a incluir en los sistemas comunes de información para la prevención del fraude en el seguro, la redacción dice así:

*2. Los datos contenidos en el sistema serán los necesarios, idóneos y proporcionales para el cumplimiento de la finalidad a la que se refiere el apartado anterior. **En caso de que se tratase de daños personales, únicamente se incorporarán al sistema los datos meramente identificativos del perjudicado, sin incluir dato alguno referente a su salud***

Esta frase deja traslucir, en opinión de esta Agencia, un error de concepto, puesto que el mero hecho de que se incorporen al sistema los datos identificativos de quien ha sufrido un *daño personal* es ya en sí mismo un “dato relativo a la salud”, pues de acuerdo con la definición contenida en el art. 4.15 RGD, en relación con el considerando 35, «datos relativos a la salud» son 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 Considerando 35 citado es muy expresivo:

*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.*

El Tribunal de Justicia de la Unión Europea (TJUE) ha entendido que el RGD contiene un concepto “amplio” de dato sensible, y en especial, de la posibilidad de existencia de datos indirectos o cruzados. Así, véanse, por ejemplo, apartados 125 y 127 de la STJUE de 1 de agosto de 2022, C- 184/20, y específicamente el apartado 127 :

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).*

(...)

127 *Por consiguiente, no cabe interpretar tales disposiciones en el sentido de que el tratamiento de datos personales que puedan desvelar indirectamente informaciones sensibles sobre una persona física queda fuera del régimen de protección reforzado establecido por las mencionadas disposiciones, pues de quedar fuera se menoscabaría el efecto útil de ese régimen y la protección de las libertades y de los derechos fundamentales de las personas físicas que pretende garantizar.*

En consecuencia, en este apartado del art. 149.2, al referirse a que una persona que ha sufrido un daño personal puede incluirse en el citado sistema, estaríamos ante tratamientos de datos de salud, lo que conlleva de nuevo la determinación en el precepto no sólo de la base jurídica de su tratamiento conforme al art. 6.1 RGPD (lo que ya se hace en el apartado 1, segundo párrafo, del art. 149 APL) sino establecer en el precepto cuál es la circunstancia del art. 9.2 RGPD que levanta la prohibición del tratamiento. En definitiva, corresponde al prelegislador establecer si la constancia de un dato de salud como el citado en los sistemas comunes para la prevención el fraude podría ser proporcional al objetivo perseguido con el registro, idóneo y necesario a tal fin, y además establecer las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

6. El art. 149.5 del APL dice:

*La información contenida en los sistemas de prevención del fraude podrá ser comunicada a las Fuerzas y Cuerpos de Seguridad, así como a los Órganos de las Administraciones Públicas de las que los mismos dependen para el ejercicio de sus funciones en la prevención y lucha contra el fraude, a fin de que por aquéllos sea posible contrastar los datos del sistema con los que consten en las denuncias que se hubieran formulado como consecuencia del siniestro. Esta comunicación es necesaria para garantizar el cumplimiento de una misión de interés público y el ejercicio por los cesionarios de sus poderes públicos, y por tanto se ampara en el artículo 6.1 e) del Reglamento (UE) 2016/679, de*

*27 de abril, en conexión con lo establecido en el artículo 100 de la Ley 20/2015, de 14 de julio.*

*Igualmente, la Dirección General de Tráfico podrá acceder a los datos contenidos en los sistemas de información con el objetivo de prevenir el fraude y la verificación de los datos contenidos en el Registro de Vehículos, amparándose asimismo el acceso en el artículo 6.1 e) del Reglamento (UE) 2016/679, de 27 de abril.*

Este precepto establece, por tanto, una comunicación, es decir, un tratamiento de datos, establecida por la ley, de unos datos contenidos en unos ficheros comunes de las aseguradoras, obtenidos por estas para prevenir el fraude en el seguro, a organismos públicos cuyas funciones son igualmente la prevención y lucha contra el citado fraude.

Esta Agencia cree oportuno recordar aquí la doctrina del Tribunal Constitucional contenida en la sentencia STC 17/2013, de 31 de enero, FJ 7, según la cual, dicho acceso ha de ser *“un acceso específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo o indiscriminado”, o “tal acceso solamente puede producirse cuando ese dato resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen legal que le resulta de aplicación”*. Esta Agencia considera que estos principios deberían de recogerse en el tratamiento de datos (la comunicación) que prevé dicho precepto.

Del mismo modo, se considera que el precepto debería de estar redactado en modo activo, y no en voz pasiva, para reforzar la idea de que los órganos de la Administración cuya función es la luchan contra el fraude son quienes podrán requerir dicha información, precisamente para luchar contra el fraude en el seguro, por ser esta la finalidad para la que se obtuvo la información que consta en el sistema (pues en caso contrario entraría en juego el art. 6.4 RGPD en vez del art. 6.3 RGPD). Dicha redacción podría ser la siguiente, o similar:

*Las Fuerzas y Cuerpos de Seguridad, así como los Órganos de las Administraciones Públicas de las que los mismos dependen, para el ejercicio de sus funciones en la prevención y lucha contra el fraude en el seguro, podrán requerir a los sistemas comunes de información para la prevención de fraude regulados en este artículo la información contenida en dichos sistemas con la finalidad de poder contrastar los datos del sistema con los que consten en las denuncias que se hubieran formulado como consecuencia del siniestro. Dicha solicitud de comunicación deberá ser de carácter específico en cada caso, ajustado a los datos que resulten precisos para la tramitación de un expediente determinado, sin que pueda tratarse de un acceso masivo o*



*indiscriminado. Dicho tratamiento de datos se realizará, en todo caso, de acuerdo con la normativa de protección de datos que sea aplicable a dicho tratamiento.*

Por otra parte, y en cuanto a su contenido material, se reitera aquí lo expuesto en el epígrafe anterior: de conformidad con el art. 149.2 del APL, los datos contenidos en esos ficheros de prevención del fraude podrían contener datos sensibles, de salud, por lo que la previsión legal del tratamiento de la cesión a las autoridades que se prevé en el apartado 5 del art. 149 debería de prever, previo el análisis correspondiente, igualmente, no sólo la base jurídica del tratamiento conforme al art. 6.1 RGPD, sino asimismo la circunstancia que, conforme al art. 9.2 RGPD, levanta la prohibición de tratamiento de datos sensibles, lo que no se expresa, así como las medidas adecuadas y específicas.

En cualquier caso, no resulta del texto del APL en este punto, si dicho tratamiento de datos personales por las FyCSE u otros órganos dedicados a la prevención del fraude, cuando se habla de *“denuncias que se hubieran formulado como consecuencia del siniestro”* se está refiriendo a actuaciones en el ámbito penal (*“denuncias”*), en cuyo caso la norma legitimadora del tratamiento podría no ser el RGPD y la LOPDGDD, sino 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, derivada de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, que regula dichos tratamientos en su art. 13, cuestión esta que debería de ser aclarada, puesto que los requisitos necesarios para el tratamiento por las autoridades de datos personales para cuestiones *“penales”* son diferentes a las reguladas por el RGPD (véase a este respecto la STJUE de 26 de enero de 2023, C-205/21, apartados 63 y 67).

7. El art. 150.5 del APL establece:

*5. Las entidades aseguradoras deberán, con carácter previo a la creación de sistemas comunes de información, dar cumplimiento a las obligaciones de responsabilidad proactiva establecidas en el artículo IV del Reglamento (UE) 2016/679, de 27 de abril. A tal efecto, las entidades aseguradoras podrán adoptar códigos de conducta reguladores de los citados sistemas comunes de información para su sometimiento a lo dispuesto en el citado reglamento y en la Ley Orgánica 3/2018, de 5 de diciembre.*

*En este caso, se considerará cumplido el deber de llevar a cabo el análisis de riesgos y, en su caso, la evaluación de impacto en la protección de datos personales respecto del funcionamiento de los sistemas comunes en caso de que los citados códigos de conducta sean aprobados por la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 38 de la Ley Orgánica 3/2018, de 5 de diciembre.»*

No se expone en la MAIN ni en el propio texto del APL de dónde en el RGPD o la LOPDGDD surge que “se entiende cumplido el deber de llevar a cabo el análisis de riesgos y, en su caso, la evaluación de impacto en la protección de datos personales respecto del funcionamiento de los sistemas comunes en caso de que los citados códigos de conducta sean aprobados por la Agencia Española de Protección de Datos”, cuando el análisis de riesgos y la EIPD es en primer lugar una actividad previa esencial para su aprobación (véase SAN 5 de diciembre de 2023, PO 1423/2021), pero en cualquier caso el RGPD no establece la falta de necesidad de llevar a cabo el análisis de riesgos o la EIPD en caso de aprobación del código. Bien al contrario, el art. 40 RGPD, referido precisamente a la EIPD, establece la obligación en su apartado 1 de que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, mientras que el apartado 10 establece la posibilidad de una excepción cuando en el curso del proceso normativo se hubiera llevado a cabo esta, no estableciéndose ninguna excepción adicional como la prevista en el apartado del APL ahora comentado. Es más, del apartado 8 del art. 35 RGPD se deduce que habrá de llevarse a cabo dicha EIPD aun en estos casos de códigos de conducta, puesto que señala:

*8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.*

En definitiva, debería de suprimirse el segundo párrafo del art. 150.5 del APL.

## II

Para finalizar, se ha aportado por el órgano proponente del APL un documento denominado Evaluación de Impacto para la protección de datos a efectos del presente APL.

Dicho documento no es en sí mismo una EIPD, ya que no cumple con el contenido que ha de tener dicha EIPD conforme al art. 35.7 RGPD, pero, a mayor abundamiento, dicho documento se refiere, de manera expresa y exclusivamente, al Fichero Informativo de Vehículos Asegurados (FIVA), y no a ningún otro tratamiento de datos del elenco amplio de tratamientos regulados en el APL, por lo que no puede ser la EIPD de esta, ni a la que se refiere el Consejo de Estado en su escrito de 18 de marzo de 2024.

En cualquier caso, y tal y como resulta del art. 35.10 RGPD, en el ámbito del procedimiento legislativo la realización de una EIPD se configura en principio sólo como una posibilidad que permite al responsable del tratamiento no realizar esta, como estaría obligado conforme al propio art. 35.1 RGPD (véase STJUE de 21 de marzo de 2024, C-61/22, apartado 66). Por ello esta AEPD “recomienda” que se lleve a cabo dicha EIPD en el seno del procedimiento legislativo en tanto en cuanto no exista una norma en derecho nacional que establezca esta como obligatoria en el seno de dicho procedimiento normativo (véase nuestro Informe 37/2023 sobre este mismo APL).

La MAIN, por otra parte, recoge el nuevo Título V del TR en el APL referido a la protección de datos en los tratamientos en materia de seguros de circulación de vehículos, pero no se menciona un análisis de riesgos o EIPD en esta materia de protección de datos.

Por último, se reiteran las observaciones realizadas en el Informe de esta AEPD 37/2023.