

**I**

Este Gabinete Jurídico viene destacando reiteradamente, en los distintas consulta sometidas a su informe, el cambio de paradigma que ha supuesto la plena aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (RGPD), en cuanto basado en el principio de “accountability” o responsabilidad proactiva, tal y como se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): *“la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”*.

En consecuencia, en virtud de dicho principio, el responsable del tratamiento deberá aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

Dentro de los diferentes instrumentos previstos por el propio RGPD para garantizar el cumplimiento de dicho principio se encuentran los códigos de conducta, ya previstos en la normativa anterior como mecanismo de autorregulación tendente a facilitar el cumplimiento de la normativa en materia de protección de datos personales. A este respecto, el Grupo del 29, en su documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios, aprobado el 10 de septiembre de 1998 (WP13), ya había venido definiendo los elementos esenciales de los mismos, destacando que los códigos debían tener la suficiente claridad y coherencia interna y proporcionar un valor añadido suficiente, en términos de estar suficientemente centrados en las cuestiones y problemas específicos de protección de datos en la organización o sector para el que se pretende aplicar y ofrecer soluciones suficientemente claras para aquellas preguntas y problemas, facilitando, en la medida en que sea posible, ejemplos de buenas prácticas, preparándose, preferiblemente, en consulta con los interesados afectados o sus

representantes. De este modo, el requisito esencial de los códigos es el de aportar un “auténtico valor añadido”, como recordaba el GT29 en su Dictamen 02/2015 sobre el Código de conducta para la computación en nube del CSIG.

Estos principios se recogen explícitamente en el RGPD, especialmente en sus Considerandos 77, 81, 98 y 99. Asimismo, el reconocimiento de los códigos de conducta como instrumento para demostrar el cumplimiento de las obligaciones de responsables y encargados se recoge en el artículo 24.3, al señalar que “La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento” y en el artículo 35.8, al disponer que “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”.

Dado el trascendente papel que desarrollan los códigos de conducta y su aplicación directa, el RGPD procede, de una manera mucho más detallada que la contenida en el artículo 27 de la Directiva 95/46/CE, a la regulación de su naturaleza, contenido, aprobación y supervisión en los artículos 40 y 41.

Dicha regulación debe completarse con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que dedica a los códigos de conducta el artículo 38, refiriéndose asimismo a ellos, como elemento de identificación de mayores riesgos del tratamiento, en el artículo 28.2.h). También destaca el papel de órgano colaborador con las autoridades de protección de datos de los organismos supervisores de los códigos de conducta en la elaboración de los planes de auditoría en el artículo 54 y en la admisión a trámite de las reclamaciones en el artículo 65.

Desde el punto de vista competencial, el artículo 28, letras f) y h), del Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio, atribuye a la Subdirección General de Promoción y Autorizaciones “Alentar la elaboración de códigos de conducta y dictaminar y proponer a la Presidencia la aprobación de los que proporcionen suficientes garantías con arreglo al artículo 40.5 del RGPD, conforme a su artículo 57.1 m)” y “Proponer a la Presidencia la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 [...] en virtud de su artículo 57.1.q)”.

En cuanto a los aspectos procedimentales, el citado artículo 38 de la LOPDGDD, en su apartado 6 prevé que “mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta”, desarrollo reglamentario que todavía

no se ha producido, por lo que deberán aplicarse, subsidiariamente, los principios generales establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en la medida en que no contradiga, se oponga, o resulte incompatible con lo dispuesto en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018.

El papel de los códigos de conducta y su vinculación con el principio de responsabilidad proactiva, en cuanto medio para acreditar el cumplimiento del RGPD, de lo que deriva la necesidad de revisar todos los códigos anteriormente aprobados, se recoge en las Directrices del Comité Europeo de Protección de Datos 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento 2016/679, destacando, asimismo, el beneficio que pueden suponer para las autoridades supervisoras al permitirles obtener una mejor comprensión y conocimiento de las actividades de tratamientos de datos de una industria, profesión u otro sector específico. Dichas directrices identifican algunos de los ámbitos en los que pueden ser útiles los códigos de conducta, como el tratamiento justo y transparente, intereses legítimos, seguridad y protección de datos desde el diseño y por defecto y obligaciones del responsable del tratamiento, partiendo de que los códigos pueden tener un alcance más amplio o más reducido, según corresponda al sector en particular, sin que sea necesario abarcar el cumplimiento de toda la legislación. Asimismo, identifica elementos de su contenido que pueden ayudar a darles un valor añadido, como el establecimiento de guías detalladas para las actividades de tratamiento específicos, mejores prácticas, soluciones prácticas a problemas identificados en un sector específico, toma en consideración de las preocupaciones del público en general o percibidas dentro del propio sector, etc.

Asimismo, las citadas Directrices detallan los criterios que deben ser tenidos en cuenta por las Autoridades de control para la aprobación de los códigos:

- 1) Que satisface una necesidad particular de ese sector o actividad de procesamiento, siendo las soluciones propuestas beneficiosas no sólo para los responsables sino también para los afectados.
- 2) Que facilita la aplicación del RGPD, identificando necesidades específicas (por ejemplo, adaptando la terminología del sector).
- 3) Que especifica la aplicación del RGPD, centrándose en los problemas del sector y aportando valor añadido, sin limitarse a reproducir los preceptos del RGPD.
- 4) Que proporciona mecanismos efectivos para controlar el cumplimiento del Código, tanto en cuanto a estructuras como procedimientos, siendo obligatorio, salvo en el caso de autoridades y organismos públicos, la existencia de un organismo de supervisión acreditado.

Para la adaptación de los códigos tipo actualmente inscritos conforme a la normativa anterior, debe estarse a lo señalado en la disposición transitoria segunda de la LOPDGDD:

Disposición transitoria segunda. Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica. Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Por consiguiente, este Gabinete Jurídico considera que, en el momento en que se proceda a la aprobación de un nuevo código de conducta o a la adaptación de un código tipo ya inscrito, dada la importancia adquirida por los códigos de conducta como consecuencia de la introducción del principio de responsabilidad proactiva, se debe ser especialmente riguroso en cuanto al contenido del mismo, que debe aportar un “auténtico valor añadido” en los términos anteriormente señalados, así como en la valoración de la suficiencia de las garantías adecuadas necesarias para su aprobación.

Por último, en relación con los organismos de supervisión de los códigos de conducta a los que se refiere el artículo 41 del RGPD, deberán cumplirse los criterios de acreditación aprobados por la Agencia Española de Protección de Datos de acuerdo con el Dictamen 1/2020 del CEPD.

## **II**

En cuanto a los requisitos de admisibilidad, deben analizarse las siguientes cuestiones:

### **a) Justificación de la necesidad del código de conducta:**

De acuerdo con el artículo 40 del RGPD, los códigos de conducta tienen por finalidad contribuir a la correcta aplicación del RGPD, debiendo acreditarse en la documentación aportada, de acuerdo con las Directrices 1/2019, la justificación y la base para la aprobación del código, describiendo la idoneidad de las salvaguardas y mecanismos propuestos.

En el presente caso, la elaboración del código de conducta se realiza al amparo de la previsión contenida en la Disposición transitoria segunda de la LOPDGDD, con la finalidad de adaptar al RGPD los tres Códigos Tipo referidos al tratamiento de datos personales en los distintos sistemas comunes de información que estaban inscritos en el Registro General de Protección de Datos de esta AEPD (Código Tipo de Fichero Histórico de Seguros del Automóvil, Código Tipo de Fichero de Automóviles Pérdida Total, Robo e Incendios y Código Tipo del Fichero de Prevención del Fraude en Seguros de Ramos diversos).

Dicha necesidad se justifica, tal y como se recoge en el informe de la Subdirección General de Promoción y Autorizaciones, en la memoria explicativa, en la que se hace referencia a la problemática específica que presenta el tratamiento de datos personales en el sector asegurador respecto de estos sistemas comunes, que ya en su momento había justificado la elaboración e inscripción de los códigos tipo referenciados, justificándolo en los siguientes términos: *“El tratamiento de datos personales en el ámbito de la actividad del sector asegurador presenta una problemática muy concreta que ha justificado incluso la existencia de una regulación específica, contenida en el artículo 99 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (en adelante, “LOSSEAR”). En ese mismo sentido cabe hacer referencia a la Recomendación (2002)9, referida a las actividades de tratamiento de datos personales en el sector asegurador, así como a la Recomendación (2016)8, referida al tratamiento de datos de salud y genéticos en el marco de la actividad aseguradora, ambas adoptadas por el Comité de Ministros del Consejo de Europa”*.

Asimismo, se hace referencia a que la *“memoria explica que el código de conducta unifica el régimen de los tres sistemas de información regulados por los códigos tipo mencionados, adaptando el tratamiento a las obligaciones derivadas del nuevo marco normativo, sistematizando las previsiones que son aplicables a todos ellos y recogiendo las especialidades que puedan ser aplicables, en concreto, a cada sistema de información”*.

Esta Gabinete Jurídico comparte la necesidad del presente Código de Conducta, valorando positivamente la elaboración de un único Código en el que se recoja conjuntamente el régimen aplicable los sistemas de información existentes en el sector asegurador y las especialidades de cada uno de ellos, al contribuir a dotar de mayor seguridad jurídica a los tratamientos de datos personales que se realizan en estos sistemas cuya existencia ha sido prevista por el propio legislador. De este modo, se garantiza que estos sistemas, que ya habían sido informados favorablemente por este Gabinete Jurídico (pudiendo citar los informes 6/2009 y 3/2016 respecto del Código Tipo relativo al Fichero Histórico de Seguros del Automóvil; los informes 1/2011 y 2/2016 referentes al Código Tipo de fichero de Automóviles de Pérdida Total, Robo e Incendios o el informe 1/2017 referente al Código Tipo del fichero de prevención del fraude en

seguros de ramos diversos) continúen cumpliendo con su finalidad con pleno respeto de lo previsto en la normativa vigente sobre protección de datos de carácter personal.

**b) Legitimación, representatividad y requisitos de la solicitud:**

El artículo 40.1 del RGPD, en su apartado 2, reconoce legitimación para promover códigos de conductas a “las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento”: De acuerdo con la Directrices 1/2019, para valorar la representatividad puede atenderse, entre otros criterios, al número o porcentaje de posibles responsables o encargados del tratamiento, representativos de un determinado sector de actividad, que puedan adherirse al código y a la experiencia del órgano representativo en relación con el sector específico y las actividades de tratamiento que sean objeto del código.

De acuerdo con su Estatutos, UNESPA se constituye como una asociación profesional de empresarios constituida al amparo de lo dispuesto en la Ley 19/1977 de 1 de abril, para la representación, gestión y defensa de los intereses profesionales, sociales y económicos comunes de sus asociados (artículo 1), pudiendo ser socios de número las entidades autorizadas para operar como aseguradoras o reaseguradoras y socios adheridos las organizaciones, asociaciones y organismos públicos y privados, siempre que en ambos casos la solicitud de incorporación sea aceptada por la Asociación (artículos 6 y 7) y que tiene por objeto: a) Representar, gestionar y defender los intereses profesionales, económicos y sociales comunes a las entidades asociadas ante toda clase de personas, organismos y organizaciones públicas o privadas, nacionales e internacionales, con pleno respeto a los principios de libertad de empresa y libre competencia. b) Representar los intereses colectivos de los asociados en materia laboral de acuerdo con la normativa vigente. c) Establecer y facilitar servicios de interés común para sus asociados. d) Colaborar con las administraciones públicas y con cualesquiera otras instituciones públicas o privadas, nacionales o internacionales, en todos aquellos asuntos que afecten al sector asegurador. e) Administrar sus propios recursos, aplicándolos a los fines y actividades previstos en estos estatutos. f) Desarrollar cualquier otra función necesaria o conveniente para la defensa de los intereses del sector y el cumplimiento de los fines de la Asociación (artículo 5).

Conforme consta en la memoria y en el Informe de la SGPA, UNESPA es la asociación empresarial que engloba a la mayor parte de las entidades del sector asegurador (98%).

Por consiguiente, la asociación promotora del código cumple los requisitos de representatividad exigidos por el RGPD.



Por otro lado, en cuanto a los requisitos formales que debe revestir la solicitud, se ha cumplido adecuadamente con los mismos, ya que constan en el expediente, además del proyecto de Código de Conducta:

- Memoria Explicativa (doc. 3)
- Estatutos de UNESPA (doc. 4)
- Certificado del acuerdo adoptado por el Comité Ejecutivo de UNESPA, en su reunión celebrada el día 5 de diciembre de 2019, en relación con el código (doc. 5)
- Escritura de apoderamiento a la Secretaria General de UNESPA (doc.6)

c) Ámbito de aplicación subjetivo y material.

El código de conducta identifica de manera clara y precisa los tratamientos de datos personales a los que resultará de aplicación, que se limitan a los tratamientos de datos personales que puedan realizarse por las entidades aseguradoras habilitadas para operar en España en alguna de las líneas de negocio a las que se refieren los Sistemas de Información regulados por el código, y que podrán adherirse a uno, dos o a los tres Sistemas que regula.

En cuanto al ámbito material, se concreta en los tratamientos de datos personales que se realizan en aquellos supuestos en que se ven obligadas a intercambiar información al objeto de garantizar el pleno cumplimiento de la normativa del seguro, estableciendo las reglas de funcionamiento de los tres Sistemas de Información en lo que afecta al cumplimiento de las normas de protección de datos.

d) Ámbito de aplicación territorial y autoridad de control competente.

El código limita su aplicación a los tratamientos de datos personales que se lleven a cabo por las entidades aseguradoras autorizadas para operar en España en relación con los tratamientos llevados a cabo en España con pleno sometimiento a lo dispuesto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras y las restantes normas aplicables a la actividad aseguradora, por lo que tiene un ámbito territorial de aplicación exclusivamente español, y como se señala en el Informe de la Subdirección General de Promoción y Autorizaciones, tiene un ámbito exclusivamente nacional, que no requiere la aplicación del mecanismo de coherencia previsto en el RGPD, siendo la autoridad competente para la aprobación del código la AEPD.

d) Consulta a las partes interesadas:

En la Memoria explicativa se justifica la ausencia de este trámite, conforme a las Directrices 1/2019 del CEPD, en los siguientes términos: “Dado el volumen de pólizas suscritas en los ramos a los que se refiere el Código de Conducta y la inexistencia de asociaciones que pudieran contar con una representación adecuada no se ha llevado a cabo el trámite de audiencia pública del Código”.

En el presente caso, teniendo en cuenta las dificultades prácticas puestas de manifiesto por la asociación promotora así como que se trata de la adaptación de unos Sistemas de Información que vienen utilizándose desde hace tiempo sometidos al previo análisis y estudio por esta AEPD sin que se haya detectado una especial problemática respecto de su aplicación, puede entenderse justificada dicha omisión.

No obstante, debe reiterarse la necesidad de que siempre que sea posible, se realice dicho trámite de audiencia, teniendo su omisión un carácter excepcional que debe ser debidamente justificado.

### III

En cuanto al contenido del código de conducta, el RGPD ha identificado determinados ámbitos que el mismo puede abarcar en el artículo 40.2:

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

- a) el tratamiento leal y transparente;
- b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
- c) la recogida de datos personales;
- d) la seudonimización de datos personales;
- e) la información proporcionada al público y a los interesados;
- f) el ejercicio de los derechos de los interesados;
- g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
- h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;
- i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;



j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

En este punto, hay que destacar que el RGPD no identifica un contenido mínimo de los códigos de conducta, sino que se trata de una relación enunciativa de materias sobre las que podrán versar los mismos y que no agota todos los supuestos que puedan plantearse para facilitar la aplicación del RGPD, a diferencia de lo que se hacía en el Reglamento de desarrollo de la LOPD de 1999, que exigía que los códigos tipo incluyeran el contenido al que se hacía referencia en el artículo 73 del Reglamento de la LOPD, que implicaba todo el ciclo de vida de los datos personales, un procedimiento de supervisión y una relación de adheridos, conforme a lo que disponían los artículos 75 y 76. Además, cabía la opción de incluir compromisos adicionales.

Lo que sí han de incluir obligatoriamente son los mecanismos de supervisión de su cumplimiento tal y como exige el artículo 40.4 del RGPD al objeto de permitir al organismo de supervisión efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo.

En consecuencia, sea cual sea el contenido material de los códigos de conducta no pueden obviar incluir los mecanismos para el control de su cumplimiento, ya se trate de códigos aplicables a responsables o encargados del sector privado, como a los promovidos por autoridades y organismos públicos.

Por consiguiente, el análisis del contenido del código de conducta al objeto de su aprobación no vendrá determinado por el mayor o menor alcance del mismo, sino por la medida en que el mismo contribuya a la mejor aplicación de la normativa de protección de datos personales, aportando un “auténtico valor añadido” y garantías suficientes, según lo indicado al principio de este informe.

En relación con el contenido, tal y como ya se ha adelantado, el código procede a la regulación de los tres sistemas de información que previamente habían sido regulados en Códigos Tipo independientes, incluyendo a lo largo de su articulado, además de los aspectos de carácter general (objeto, ámbito de aplicación, entrada en vigor, modificación, difusión y formación) su gobernanza, las normas aplicables a todos los Sistemas y las especialidades de cada uno de ellos, estructurándose en cuatro partes:

- Parte 1. Aspectos generales del Código de Conducta.
- Parte 2. Gobernanza del Código de Conducta.
- Parte 3. Normas de funcionamiento comunes aplicables a los sistemas de información regulados por este Código.
- Parte 4. Especialidades de cada Sistema de Información.

De este modo, presenta un contenido muy amplio que, en relación con estos Sistemas de Información, abarca la práctica totalidad de los supuestos identificados en el artículo 40.2. del RGPD, dada su intención de facilitar a las entidades adheridas el respeto de la normativa sobre protección de datos personales en el cumplimiento de sus obligaciones legales.

El informe de la Subdirección General de Promoción y Autorizaciones realiza un análisis exhaustivo del contenido del código de conducta atendiendo a la propia estructura del mismo en su apartado IV. B), para concluir en su apartado IV.C) que el mismo cumple con los criterios necesarios para su aprobación:

### **C) VALORACIÓN**

Con carácter previo a la valoración de las características del código de conducta, cabe tener presente el considerando 98 del RGPD que insta a incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta que, respetando sus límites, faciliten su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo por los distintos sectores de tratamiento de datos.

Del análisis del contenido del código cabría indicar que con carácter general se ajustaría a los criterios que para su aprobación se recogen en las Directrices 1/2019 del CEPD, cuyo objetivo es que los códigos puedan demostrar que contribuyen a la adecuada aplicación del RGPD. En concreto, se debe demostrar que el código de conducta:

#### **1. Responde a necesidades particulares para las actividades de tratamiento de datos personales**

La actividad del sector asegurador, como se recoge en la memoria de presentación del código de conducta, presenta unas características específicas que se recogen en la legislación sectorial que la regula, a la que se ha hecho referencia anteriormente, y que afecta a los tratamientos de datos que se realizan por las entidades del sector en el ejercicio de su actividad.

Características que en su momento motivaron la elaboración de códigos tipo para aplicar la normativa de protección de datos a las necesidades del sector, que en el ámbito que regula el código se centran en el cumplimiento de las obligaciones que la legislación específica impone a

las entidades adheridas como son las de adoptar medidas efectivas para prevenir, impedir, identificar, detectar, informar y remediar conductas fraudulentas relativas a seguros, para lo que se prevé la adopción de ficheros comunes sin que sea necesario el consentimiento de los afectados (LOSSEAR).

En ese sentido, la finalidad de la valoración del riesgo asegurado y la oportunidad de llevar a cabo el aseguramiento solicitado, así como la cuantificación de la prima, son finalidades que presentan necesidades específicas en cuanto al tratamiento de datos personales en los Sistemas de Información creados para cumplirlas.

El código define la finalidad de los tratamientos de datos de cada uno de los Sistemas de Información: la realización de una valoración técnica y objetiva del riesgo, así como la correcta aplicación de las tarifas de prima en el Sistema SIHSA; y la prevención del fraude en los Sistema SIAPTRI y SIPFSRD.

Por tanto, en la medida que el código se dirige a regular estos aspectos de los tratamientos de datos que realiza el sector asegurador para el cumplimiento de las finalidades que señala, respondería a necesidades específicas del sector asegurador representado por el promotor del código.

## **2. Facilita y especifica la aplicación del RGPD**

El código contiene una regulación práctica de cómo se ha de aplicar el RGPD en los Sistemas Comunes de Información, que responde a las necesidades específicas del sector, proporciona un valor añadido a la normativa aplicable y facilita su aplicación por el sector.

En este sentido, la aclaración de la posición de las entidades aseguradoras que se adhieran al código como corresponsables del tratamiento de los datos personales y el acuerdo de corresponsabilidad, abandonando la posición recogida en los códigos tipo anteriores al RGPD, en el que el promotor también era responsable de los ficheros comunes.

Así mismo, la definición de la finalidad de cada uno de los Sistemas de Información, la base jurídica del tratamiento de los datos personales, la aplicación práctica de los principios de protección de datos, de la atención al ejercicio de derechos y de las quiebras de seguridad constituyen un valor añadido que contribuye a facilitar el cumplimiento del RGPD y de la normativa nacional aplicable.

Esta consideración se puede predicar de la inclusión de los terceros cesionarios y la legitimación para las cesiones de los datos: las Fuerzas y Cuerpos de Seguridad del Estado, Administración de Justicia y la Dirección General de Tráfico.

Si bien la inclusión de un apartado para las definiciones de los conceptos específicos del sector asegurador como póliza, prima, siniestro, tomador, beneficiario, perjudicado, hubiera contribuido a especificar la aplicación del código, ello no impide realizar una valoración global favorable de este aspecto.

## **3. Aporta garantías suficientes**

El artículo 40.5 del RGPD estipula que los códigos de conducta se aprobarán sólo si aportan suficientes garantías adecuadas. A su vez, las Directrices del CEPD recogen que los promotores deberán demostrar ante la autoridad de control competente que su código contiene garantías suficientes y eficaces para mitigar el riesgo que entraña el tratamiento de datos y para respetar los derechos y las libertades de los particulares.

La aplicación de los principios de protección de datos, como el de transparencia, minimización, exactitud, finalidad y conservación ofrecen garantías adecuadas y suficientes para los derechos y libertades de los afectados.

La prohibición de la adopción de decisiones personales automatizadas y de realizar perfilados, la selección del encargado del tratamiento y la asignación que en nombre de los responsables se le atribuyen en el código y que se han de reflejar en el contrato de encargo de tratamiento, proporcionan igualmente garantías adecuadas. La designación de TIREA como encargado del tratamiento también resultaría una garantía en cuanto al establecimiento, mantenimiento y actualización de las medidas técnicas y organizativas para garantizar los derechos y libertades de los afectados.

Finalmente, el establecimiento de un procedimiento voluntario y gratuito de resolución extrajudicial de las controversias que, al margen de las ocasionadas por el incumplimiento del código, puedan surgir por la vulneración del RGPD o la LOPDGPDD, y cuya resolución dictada por el Comité Técnico del OCCC son de obligado cumplimiento para la entidad adherida, formaría también parte de las garantías que aporta el código.

#### **4. Proporciona mecanismos efectivos de supervisión de cumplimiento del código**

Los mecanismos de supervisión que incluye el código se relacionan en el apartado IV.5 de este informe, al que debemos remitirnos. El conjunto de todos ellos puede satisfacer la obligación de disponer de recursos para supervisar y controlar el cumplimiento del código, mediante acciones preventivas, determinando la adhesión de las entidades, de formación, información y asesoramiento; acciones de vigilancia y control de su cumplimiento y potestades sancionadoras en caso de incumplimiento por alguna de las entidades adheridas.

Este Gabinete Jurídico coincide en dicha valoración positiva. Tal y como se ha señalado ya al tratar la necesidad del código, el mismo se configura como un elemento muy relevante para dotar de seguridad jurídica al tratamiento de datos personales en los Sistemas de Información empleados en el sector asegurador, y se adecua a los criterios que se han venido sosteniendo por esta Agencia, adaptando adecuadamente la autorregulación existente a los criterios, principios y obligaciones de la vigente normativa sobre datos de carácter personal.

De este modo, desde una perspectiva jurídica, debe concluirse que el contenido del código de conducta se adecúa a las disposiciones del RGPD y la LOPDGDD, y que el mismo aporta un “auténtico valor añadido” en los términos que se vienen analizando en el presente informe, así como incorpora las garantías adecuadas necesarias para su aprobación.

A este respecto, interesa destacar las siguientes cuestiones que, en relación con los Sistemas de Información, son tratadas adecuadamente en el código de conducta:

#### 1. Posición jurídica de los participantes.

El código de conducta modifica la atribución de responsabilidades que se contenía en los códigos tipo, en los que la propia promotora se constituía como responsable del fichero, que era la que suscribía el contrato de encargo del tratamiento con TIREA, mientras que las entidades aseguradoras y el Instituto de Investigación sobre Reparación de Vehículos, S.A. (Centro Zaragoza, que actúa por delegación de las entidades aseguradoras) serían las entidades usuarias del fichero.

La correcta aplicación de la normativa sobre protección de datos personales exige una correcta identificación de la posición jurídica que asume cada uno de los intervinientes en el tratamiento de los datos personales, con el objeto de determinar con acierto la atribución de responsabilidades en relación con dicho tratamiento.

La importancia de dicha identificación es puesta de manifiesto por el propio RGPD en su Considerando 79:

(...)La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable (...).

No obstante, dicha atribución de responsabilidades, de marcado carácter funcional, no siempre resulta una tarea fácil, como pone de manifiesto las dudas y las numerosas consultas que, al respecto, se reciben en esta Agencia.

De este modo, en los distintos informes que se van emitiendo, se insiste en que esta regulación pretende que no queden supuestos de actuación fuera de su ámbito de aplicación, con el fin de dotar a las autoridades de supervisión, de los elementos necesarios para desarrollar su función y en definitiva para brindar a los ciudadanos europeos, la protección que merecen sus datos de carácter personal. Por tanto, cualquier actividad que conlleve el tratamiento de datos personales será atribuible a algún sujeto que cumpla los requisitos de las distintas categorías que ofrece el RGPD.

El RGPD define en su artículo 4.7 la figura del responsable del tratamiento o responsable como “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.”

Y en su artículo 4.8) define la figura del encargado del tratamiento o encargado como “la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”.

En este sentido debe indicarse, que la figura del encargado del tratamiento obedece a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que lleve aparejado el tratamiento de datos personales estaremos ante un tratamiento realizado por cuenta del responsable.

Lo que no implica necesariamente que los datos objeto de tratamiento, sean titularidad del responsable, sino que las operaciones de tratamiento, entre las que se encuentra, por ejemplo la recogida, se atribuyan al responsable.

Esto significa que el tratamiento de los datos se realiza por el encargado en nombre del responsable como si fuera este mismo quien lo lleva a cabo.

Como otra manifestación del principio de responsabilidad proactiva, el RGPD impone al responsable del tratamiento, una obligación de diligencia a la hora de elegir un encargado de tratamiento al indicar en el Considerando 81 lo siguiente(...)Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y



organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento.(...).

En cuanto al soporte formal de la relación entre responsable y encargado, el artículo 28 del RGPD exige en su apartado tercero la existencia de un contrato u otro acto jurídico con arreglo al derecho de la Unión o de los Estados miembros que vincule al encargado respecto del responsable. Contrato o acto jurídico que deberá constar por escrito, inclusive en formato electrónico, como señala el apartado 9 de dicho artículo.

Entre las determinaciones que debe contener dicho contrato se recoge en primer lugar la estipulación de que el encargado "tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público" Asimismo, el número 10 del artículo 28, establece que "Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento."

Por su parte, la LOPDGDD en su artículo 33 regula la figura del encargado del tratamiento, y ofrece aclaraciones para determinar cuando estamos ante esta figura, al indicar lo siguiente:

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.
2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Como puede observarse, la LOPDGDD pretende ofrecer soluciones a supuestos que en la práctica figuran avalados por un contrato y que en la realidad responden a un falso encargado o encargo simulado, pues materialmente, la entidad contratada decide sobre el uso y finalidad del

tratamiento al establecer relaciones directas con los afectados, excediendo así de la encomienda que consta en el contrato y convirtiéndose en un responsable del tratamiento.

En cuanto a las obligaciones generales del responsable y del encargado del tratamiento, hay que tener en cuenta, además de las derivadas del cumplimiento de los principios generales previstos en el artículo 5 del RGPD, del derecho de información previsto en los artículos 13 y 14 del RGPD, y de las obligaciones derivadas del principio responsabilidad proactiva, lo dispuesto en el artículo 28 de la LOPDGDD, que indica lo siguiente:

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Como ya señalaba el Grupo del artículo 29, en su Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», el concepto de responsable era un concepto funcional dirigido a la asignación de responsabilidades, indicando que “El concepto de «responsable del tratamiento» y su interacción con el concepto de «encargado del tratamiento» desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos y la manera en que los interesados pueden ejercer sus derechos en la práctica. El concepto de responsable del tratamiento de datos también es esencial a la hora de determinar la legislación nacional aplicable y para el ejercicio eficaz de las tareas de supervisión conferidas a las autoridades de protección de datos”.

Asimismo, el citado Dictamen destacaba “las dificultades para poner en práctica las definiciones de la Directiva en un entorno complejo en el que caben muchas situaciones hipotéticas que impliquen la actuación de responsables y encargados del tratamiento, solos o conjuntamente, y con distintos grados de autonomía y responsabilidad” y que “El Grupo reconoce que la aplicación concreta de los conceptos de responsable del tratamiento de datos y encargado del tratamiento de datos se está haciendo cada vez más compleja. Esto se debe ante todo a la creciente complejidad del entorno en el que se usan estos conceptos y, en particular, a una tendencia en aumento, tanto en el sector privado como en el público, hacia una diferenciación organizativa, combinada con el desarrollo de las TIC y la globalización, lo cual puede dar lugar a que se planteen cuestiones nuevas y difíciles y a que, en ocasiones, se vea disminuido el nivel de protección de los interesados”.

No obstante, en el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha

señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Asimismo, partiendo de dicho principio de responsabilidad proactiva, dirigido esencialmente al responsable del tratamiento, y al objeto de reforzar la protección de los afectados, el RGPD ha introducido nuevas obligaciones exigibles no sólo al responsable, sino en determinados supuestos, también al encargado del tratamiento, quien podrá ser sancionado en caso de incumplimiento de las mismas.

A este respecto, las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD) sobre los conceptos de responsable del tratamiento y encargado en el RGPD hacen especial referencia (apartado 91) a la obligación del encargado de garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria (artículo 28, apartado 3); la de llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable (Artículo 30.2); la de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (artículo 32); la de designar un delegado de protección de datos bajo determinadas condiciones (artículo 37) y la de notificar al responsable del tratamiento sin dilación indebida las violaciones de la seguridad de los datos personales de las que tenga conocimiento (artículo 33 (2)). Además, las normas sobre transferencias de datos a terceros países (capítulo V) se aplican tanto a los encargados como a los responsables. Y por ello el CEPD considera que el artículo 28 (3) del RGPD impone obligaciones directas a los encargados, incluida la obligación de ayudar al responsable del tratamiento a garantizar el cumplimiento.

Sin perjuicio de la atribución de obligaciones directas al encargado, las citadas Directrices, partiendo de que los conceptos de responsable y encargado del RGPD no han cambiado en comparación con la Directiva 95/46 / CE y que, en general, los criterios sobre cómo atribuir los diferentes roles

siguen siendo los mismos (apartado 11), reitera que se trata de conceptos funcionales, que tienen por objeto asignar responsabilidades de acuerdo con los roles reales de las partes (apartado 12), lo que implica que en la mayoría de los supuestos deba atenderse a las circunstancias del caso concreto (case by case) atendiendo a sus actividades reales en lugar de la designación formal de un actor como "responsable" o "encargado" (por ejemplo, en un contrato), así como de conceptos autónomos, cuya interpretación debe realizarse al amparo de la normativa europea sobre protección de datos personales (apartado 13), y teniendo en cuenta (apartado 24) que la necesidad de una evaluación fáctica también significa que el papel de un responsable del tratamiento no se deriva de la naturaleza de una entidad que está procesando datos sino de sus actividades concretas en un contexto específico, por lo que la misma entidad puede actuar al mismo tiempo como responsable del tratamiento para determinadas operaciones de tratamiento y como encargado para otras, y la calificación como responsable o encargado debe evaluarse con respecto a cada actividad específica de procesamiento de datos.

No obstante, en la práctica pueden darse situaciones más complejas atendiendo a las distintas funciones de los actores y al tratamiento en sí mismo considerado, y es preciso acudir a los criterios interpretativos fijados por el Comité Europeo de Protección de Datos, en las Directrices 7/2020 de 2 de septiembre de 2020 "Sobre los conceptos de responsable y encargado en el RGPD", de las que cabe destacar los siguientes apartados:

12. Los conceptos de responsable y encargado son conceptos funcionales: su objetivo es asignar responsabilidades de acuerdo con las funciones reales de las partes. Esto implica que la condición jurídica de un actor como «responsable» o «encargado» debe determinarse en principio por sus actividades reales en una situación específica, y no por la designación formal de un actor como «responsable» o «encargado» (por ejemplo, en un contrato).

21(...) En la mayoría de las situaciones, el «órgano determinante» puede identificarse fácil y claramente por referencia a determinadas circunstancias jurídicas o fácticas de las que normalmente puede inferirse la «influencia», a menos que otros elementos indiquen lo contrario. Se pueden distinguir dos categorías de situaciones: 1) el control derivado de las disposiciones legales; y (2) control derivado de la influencia fáctica. (...)

22 (...) Hay casos en que el control puede deducirse de una competencia jurídica explícita por ejemplo, cuando el responsable o los criterios específicos para su designación son designados por el Derecho nacional o de la Unión (...) el legislador ha designado como responsable a la entidad que tiene una capacidad genuina de ejercer el control

23 la ley establecerá una tarea o impondrá a alguien la obligación de recopilar y tratar determinados datos. En esos casos, la finalidad de la tramitación suele ser determinada por la ley. El responsable será normalmente el designado por la ley para la realización de este propósito, esta tarea pública (...) De manera más general, la ley también puede imponer a las entidades públicas o privadas la obligación de conservar o facilitar determinados datos. Estas entidades normalmente se considerarían responsables con respecto al tratamiento necesario para cumplir esta obligación.

25. La necesidad de una evaluación fáctica significa también que el papel de un responsable del tratamiento no se deriva de la naturaleza de una entidad que está tratando datos, sino de sus actividades concretas en un contexto específico. En otras palabras, la misma entidad puede actuar al mismo tiempo que el responsable de determinadas operaciones de tratamiento y como encargado para otras, y la calificación como responsable o encargado debe evaluarse con respecto a cada actividad específica de tratamiento de datos.

26 (...) Cuando una entidad se dedica al tratamiento de datos personales como parte de sus interacciones con sus propios empleados, clientes o miembros, generalmente será la que pueda determinar de hecho el propósito y los medios en torno al tratamiento y, por lo tanto, actúa como responsable en el sentido del RGPD (...)

27 (...) las condiciones de un contrato no son decisivas en todas las circunstancias, ya que esto simplemente permitiría a las partes asignar la responsabilidad que estimen conveniente. No es posible convertirse en responsable o eludir las obligaciones de responsable simplemente configurando el contrato de una manera determinada cuando las circunstancias de hecho dicen algo más.

28. Si una de las partes decide de hecho por qué y cómo se tratan los datos personales esa parte será un responsable, incluso si un contrato dice que es un encargado. Del mismo modo, no es porque un contrato comercial utilice el término «subcontratista» que una entidad sea considerada un encargado desde la perspectiva de la legislación de protección de datos (...)

75. Dos condiciones básicas para la calificación como encargado son:

Ser una entidad separada en relación con el responsable y Tratamiento de datos personales en nombre del responsable del tratamiento. (...)

78. El tratamiento de datos personales en nombre del responsable del tratamiento requiere, en primer lugar, que la entidad independiente procese datos personales en beneficio del responsable. En el artículo 4, apartado 2, el tratamiento se define como un concepto que incluye una amplia gama de operaciones



que van desde la recogida, el almacenamiento y la consulta hasta la utilización, difusión o cualquier otra forma de puesta a disposición y destrucción. En la práctica, esto significa que todo tratamiento imaginable de datos personales constituye tratamiento (...)

79. En segundo lugar, el tratamiento debe realizarse en nombre de un responsable, pero no bajo su autoridad o control directo. Actuar «en nombre de» significa servir a los intereses de otra persona y recuerda el concepto jurídico de «delegación». En el caso de la legislación sobre protección de datos, se pide al encargado que aplique las instrucciones dadas por el responsable del tratamiento al menos con respecto a la finalidad del tratamiento y los elementos esenciales de los medios (...)

80. Actuar «en nombre de» significa también que el encargado no puede llevar a cabo el tratamiento para su propio(s) propósito(s).

81. El EDPB recuerda que no todos los proveedores de servicios que tratan datos personales durante la prestación de un servicio son «encargados» en el sentido del RGPD. El papel de un encargado no se deriva de la naturaleza de una entidad que está tratando datos, sino de sus actividades concretas en un contexto específico. La naturaleza del servicio determinará si la actividad de tratamiento equivale al tratamiento de datos personales en nombre del responsable del tratamiento en el sentido del RGPD.

Partiendo de los criterios anteriormente señalados, y siendo el responsable del tratamiento quién determina los fines y los medios del mismo, *solo o junto con otros*, el código de conducta procede a revisar la asignación de roles para adecuarla a la normativa sobre protección de datos personales.

De este modo, siendo la base jurídica del tratamiento, tal y como posteriormente se verá, el cumplimiento de las obligaciones legales que la normativa del seguro impone a las entidades aseguradoras, a ellas les corresponde el concepto de responsables del tratamiento en cuanto sujetos obligados al cumplimiento de las mismas, y siendo necesaria la colaboración entre todas ellas para el adecuado funcionamiento de los Sistemas de Información, determinando conjuntamente los medios, esta relación se articula como un supuesto de corresponsabilidad previsto en el artículo 26 del RGPD, incluyendo un modelo de acuerdo de corresponsabilidad que deberán suscribir todas las entidades aseguradoras que se adhieran al código, lo que se considera adecuado, siendo a dichas entidades a las que les corresponde el cumplimiento de las obligaciones que la normativa sobre protección de datos personales impone a los responsables del tratamiento:

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán

considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

De nuevo, las Directrices 07/2020 del CEPD ofrecen criterios para identificar una situación de corresponsabilidad, entendiendo que “En términos generales, existe una corresponsabilidad del tratamiento concreta cuando diferentes partes determinan conjuntamente los objetivos y los medios del tratamiento” (Apartado 51) y partiendo igualmente de que “La evaluación de la corresponsabilidad debe basarse en un análisis fáctico, y no en un análisis formal, de la influencia real sobre los fines y los medios del tratamiento” (Apartado 52):

59. Existe corresponsabilidad del tratamiento cuando los entes que participan en el mismo tratamiento lo llevan a cabo para unos fines definidos conjuntamente. Esto es así cuando los entes participantes tratan los datos para el mismo fin o para un fin común.

68. Es importante subrayar que el uso de una infraestructura o un sistema de tratamiento de datos común no conlleva en todos los casos la calificación de las partes como corresponsables del tratamiento, en particular cuando el tratamiento que lleven a cabo sea independiente y pueda ser realizado por una de las partes sin la intervención de la otra o cuando el proveedor sea un encargado del tratamiento, por no perseguir ningún fin propio (la existencia de un mero beneficio comercial para las partes involucradas no es suficiente para que se considere fin del tratamiento).

Por el contrario, UNESPA, que ostenta la condición de promotora del código, carece de la condición de responsable o corresponsable del tratamiento, ya que las actuaciones concretas que a la misma corresponde en virtud del código deriva de dicha condición de promotora y de actuar, en su caso, en el ejercicio de sus funciones representativas del sector.

Por su parte, la gestión de los tres sistemas comunes de información continuará realizándose por TIREA, que mantiene la condición de encargada del tratamiento si bien lo será de cada una de las entidades corresponsables, siendo necesaria la suscripción con cada una de ellas del contrato previsto en el artículo 28.3 del RGPD y con las precisiones que se incorporan en el código, sin perjuicio del contrato que con carácter general y actuando en representación de dichas entidades aseguradoras firmará con UNESPA, que es la que le corresponde la elección, en nombre de las Entidades Aseguradoras Adheridas, de un encargado del tratamiento que ofrezca garantías suficientes y el control de la implantación por el encargado del tratamiento de las medidas de responsabilidad activa exigidas por las normas de protección de datos personales. Por consiguiente, TIREA tratará los datos personales como encargado y en virtud del correspondiente contrato, sin perjuicio de que, asimismo, se le atribuyan algunas funciones propias de los responsables, como es la notificación de las brechas de seguridad a la AEPD, lo que se justifica en la necesidad de evitar la recepción por la AEPD de reiteradas comunicaciones similares referidas a una misma quiebra de seguridad. En estos casos, estará actuando como representante del responsable del tratamiento, que es el obligado a comunicar las brechas conforme al artículo 33 del RGPD, sin que dicha representación le exima de dicha responsabilidad. Asimismo, se contempla que, en virtud de la correspondiente autorización contractual, TIREA será la encargada de atender y gestionar las solicitudes de ejercicio de derechos que puedan presentarse por los afectados, actuando, igualmente, en representación de los responsables del tratamiento.

Por otro lado, respecto del Sistema de Información de automóviles, pérdida total o robo, se contempla la posibilidad de que el Centro de Zaragoza pueda acceder a los datos como encargado del tratamiento de aquellas Entidades Aseguradoras adheridas que hayan delegado en el mismo suscribiendo el correspondiente contrato de encargo con el contenido del artículo 28.3. del RGPD, previa acreditación documental ante TIREA.

## **2. Base legitimadora del tratamiento.**

No siendo admisible como base jurídica legitimadora del tratamiento de datos personales la mera habilitación legal, siendo necesaria su identificación conforme alguno de los supuestos específicos contemplados en el artículo 6.1. del RGPD, la base jurídica viene determinada por el cumplimiento de

obligaciones legales aplicables al responsable del tratamiento (artículo 6.1. c) del RGPD), estando establecidas las correspondientes obligaciones en normas con rango de ley (artículo 8.1. de la LOPDGDD).

En particular, el Sistema de Información Histórico de Seguros del Automóvil en el que se incluirá la información del histórico de siniestros en relación con las pólizas suscritas por un tomador en los últimos cinco años, responde a la necesidad de cumplir lo exigido por el artículo 2.7 del 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, conforme al cual *“Las entidades aseguradoras deberán expedir a favor del propietario del vehículo y del tomador del seguro del vehículo asegurado, en caso de ser persona distinta de aquél, previa petición de cualquiera de ellos, y en el plazo de quince días hábiles, certificación acreditativa de los siniestros de los que se derive responsabilidad frente a terceros, correspondientes a los cinco últimos años de seguro, si los hubiere o, en su caso, una certificación de ausencia de siniestros”*, completado por el artículo 9 del Real Decreto 1507/2008, de 12 de septiembre, según el cual el cumplimiento de dicha obligación podrá realizarse *“por medio de los ficheros comunes establecidos por (las entidades aseguradoras) para la selección y tarificación de riesgos a los que se refiere el artículo 99.7 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras”*.

En cuanto a los Sistemas que tienen por finalidad la prevención del fraude, tanto el Sistema de Información de Automóviles Pérdida Total, Robo e Incendios, en el que se incluirá información referida a los siniestros objeto de cobertura en el ámbito del seguro de vehículos de motor, como el Sistema de Información de Prevención del Fraude en Seguros de Ramos Diversos, en el que se incluirá información referida a los siniestros objeto de cobertura en el ámbito de los seguros relacionados con los ámbitos de hogar, comunidades, comercios y oficinas e industrias y PYMES, son necesarios para el cumplimiento de la obligación impuesta a las entidades aseguradoras por el artículo 100 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, consistente en *“adoptar medidas efectivas para, prevenir, impedir, identificar, detectar, informar y remediar conductas fraudulentas relativas a seguros, ya se adopten de forma individual o mediante su participación en ficheros comunes”*, teniendo en cuenta que el artículo 99.7 de la misma establece que *“También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación, cancelación y oposición”*.

Por otro lado, el código prevé expresamente que no serán objeto de tratamiento categorías especiales de datos, cuyo tratamiento estaría prohibido si no concurre alguna de las circunstancias contempladas en el artículo 9.2. del RGPD.

Asimismo, el código se refiere a distintos supuestos de acceso a la información por parte de autoridades públicas en el ejercicio de las competencias legalmente atribuidas, como es el supuesto del acceso a la información de los Sistemas comunes de información contra el fraude por las Fuerzas y Cuerpos de Seguridad y los órganos de las Administraciones Públicas de las que dependen, en virtud de la colaboración prevista en el artículo 100, segundo párrafo, de la LOSSEAR: “Las entidades aseguradoras también podrán suscribir convenios de colaboración con el Ministerio del Interior y los Cuerpos y Fuerzas de Seguridad del Estado, así como con las consejerías y policías de las Comunidades Autónomas que tengan funciones análogas, con objeto de colaborar, cada uno en el ámbito de sus competencias, en la prevención e investigación del fraude en el seguro. En todo caso, el intercambio de información que pudiera llevarse a cabo al amparo de dichos convenios respetará lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre”. De este modo, el acceso queda legitimado conforme a lo previsto en la letra e) del artículo 6.1. del RGPD: “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”. Y en el supuesto de acceso por los órgano jurisdiccionales en el ejercicio de su función jurisdiccional, el mismo se encuentra amparado por el artículo 6.1.c) del RGPD como consecuencia de la obligación impuesta en la Constitución de colaborar con los Jueces y Tribunales en el ámbito de su función.

No obstante, en los supuestos expresamente contemplados en el artículo 7 de 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, el acceso a la información en virtud del deber de colaboración que el mismo establece quedará legitimado conforme a la letra c) del artículo 6.1. del RGPD, al ser necesario para el cumplimiento de una obligación legal.

Por otro lado, también se contempla el acceso al Sistema de Información de automóviles, pérdida total, robo e incendios por la Dirección General de Tráfico, en el ejercicio de las competencias que legalmente le atribuye la normativa reguladora del Tráfico, circulación de vehículos a motor y seguridad vial, al amparo de lo previsto en el artículo 6.1.e) del RGPD.

### 3. Valor añadido del código de conducta.

A lo largo de su regulación, el código de conducta, además de clarificar la aplicación del RGPD en relación con el establecimiento y funcionamiento de los sistemas de información, identificando, entre otras cuestiones, la posición jurídica de los intervinientes y las bases legitimadoras, incorpora numerosas garantías tendentes a asegurar la correcta aplicación de la normativa de protección de datos personales, como ocurre respecto de la aplicación de los principios de protección de datos contenidos en el artículo 5 del RGPD, el contenido de los contratos de encargo del tratamiento o la efectividad del ejercicio de los derechos de los afectados, incluida la prohibición de la adopción de decisiones personales automatizadas y de realizar perfilados.

Estas garantías se articulan mediante obligaciones específicas y exigibles a través de los mecanismos de control que el código establece, lo que refuerza el carácter vinculante del mismo, tal y como se destacaba en nuestro Informe 89/2020:

A este respecto, hay que partir de la configuración de los códigos de conducta como un mecanismo de autorregulación derivado de la autonomía de la voluntad y que se convierte en fuente de normas jurídicamente vinculantes para los que se adhieren voluntariamente al mismo, contribuyen, de este modo, a concretar la aplicación del ordenamiento jurídico vigente, que deberán respetar en todo momento. Por ello, entiende este Gabinete Jurídico, que la necesidad de establecer obligaciones jurídicamente exigibles es consustancial a la propia naturaleza de los códigos de conducta, vinculando a aquellos que libremente lo han suscrito. La necesidad de que los códigos de conducta tengan un contenido obligatorio deriva, asimismo, del propio RGPD y de la importante función que atribuye a los mismos respecto del cumplimiento del principio de responsabilidad proactiva. A este respecto, el artículo 40.4 del RGPD dispone que “El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56”. Por consiguiente, no son admisibles en un código de conducta las meras recomendaciones, que deben suprimirse del mismo, al no ser posible su control obligatorio. Del mismo modo, el artículo 40.3, cuando prevé la adhesión al código de responsables o encargados del tratamiento a los que no aplica el RGPD, requiere que asuman “compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas”, careciendo de sentido la exigencia un compromiso jurídicamente vinculante respecto a meras recomendaciones. En este mismo sentido, el apartado 37 de las Directrices 1/2019, se refiere a normas y reglas, lo que denota su carácter obligatorio: “Las normas y reglas acordadas



deberán ser inequívocas, concretas, asequibles y aplicables (verificables). El establecimiento de normas específicas en un ámbito concreto es un método aceptable por medio del cual un código puede aportar valor añadido. El uso de terminología única y pertinente para dicho sector y la aportación de casos o ejemplos específicos de mejores prácticas puede contribuir a cumplir este requisito”.

Por último, para concluir el análisis de determinados aspectos que contribuyen a considerar que el código aporta un auténtico valor añadido, debe hacerse especial referencia, sin perjuicio del resto del amplio contenido del código, al establecimiento de un procedimiento previo de resolución extrajudicial de controversias, de carácter voluntario y gratuito.

#### **IV**

En cuanto a los mecanismos de control del cumplimiento del código, ya se ha señalado anteriormente que deben incluirse preceptivamente en los códigos de conducta, a tenor de lo dispuesto en el artículo 40.4 del RGPD:

“El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56”.

A estos efectos, el código incluye las correspondientes medidas de control y supervisión que aplicará el organismo de supervisión y que se detallan en el informe de la Subdirección General de Promoción y Autorizaciones, entre las que destacan la de atender a las consultas de las entidades aseguradoras adheridas, la de recabar información de las entidades adheridas sobre el funcionamiento de los sistemas regulados por el código, el establecimiento de un programa anual de revisiones sistemáticas y aleatorias y la aplicación del régimen sancionador.

#### **V**

Como organismo de supervisión del código, exigible igualmente a los códigos de conducta al amparo del artículo 41 del RGPD, con excepción de los que se promuevan por autoridades y organismos públicos, se configura el denominado Órgano de Control del Código de Conducta, conteniéndose en el Informe de la Subdirección General de Promoción y Autorizaciones el análisis detallado del cumplimiento de los criterios de acreditación establecidos, previo dictamen del CEPD, por la AEPD, publicados el 27 de febrero de 2020, y que este Gabinete Jurídico comparte, por lo que puede procederse a su acreditación.

## **VI**

A la vista de todo lo analizado en el presente informe, este Gabinete Jurídico **Informa favorablemente** la aprobación, por la Agencia Española de Protección de Datos, del Código de conducta regulador del tratamiento de datos personales en los sistemas comunes del sector asegurador, presentado por la Unión Española de Entidades Aseguradoras (UNESPA) así como la acreditación del Órgano de Control del Código de Conducta como organismo de supervisión del mismo.