

N/REF: 0018/2023

La consulta plantea varias cuestiones relacionadas con el FICHERO CONFIRMA DE PREVENCIÓN DEL FRAUDE y su adecuación al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en lo sucesivo) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo).

En concreto, solicita el parecer de esta Agencia sobre el rol que deben desempeñar las Entidades Adheridas al Fichero Confirma y la consultante, Confirma Sistemas de Información, S.L. (Confirma o la consultante en lo sucesivo) tras la entrada en vigor del RGPD y la LOPDGDD; sobre la ampliación de los plazos de conservación de los datos de las solicitudes existentes en el sistema y la posible afectación al principio de exactitud; sobre la creación de un nuevo estado de las solicitudes denominado “posible suplantación de la finalidad” y la posible afectación al principio de licitud; sobre la creación de un nuevo estado temporal denominado “en revisión” y la posible afectación al principio de limitación de la finalidad; y finalmente sobre la posibilidad de consulta durante toda la vida de la operación de aquellas respecto a las que haya sospechas de fraude o comportamiento inusual.

I

Como punto de partida debe indicarse que esta Agencia emitió el Informe 150/2013 de fecha 30 de abril de 2013, sobre la adecuación del Reglamento del Fichero Confirma a la normativa de protección de datos personales vigente en aquel momento, (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD) y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RDLOPD).) dónde se describía la finalidad y el funcionamiento de este sistema de prevención y lucha contra el fraude, a cuyo tenor:

El citado Reglamento del Fichero Confirma establece las reglas de funcionamiento del fichero, debiendo tenerse en cuenta las siguientes características del mismo:

1.- Según el artículo 1 del Reglamento, relativo a definiciones, el Fichero Confirma es un fichero común de solicitudes de operaciones creado con

la finalidad de prevención del fraude; se nutre de datos facilitados por las entidades que reciben las solicitudes y por tanto contiene datos de solicitudes de operaciones que permiten la detección automática de datos irregulares.

Podrán ser “entidades usuarias o participantes” en el fichero las que realicen operaciones de financiación y puedan ser objeto de fraude en la contratación, siempre que se adhieran al Reglamento aportado.

2.- Los datos incorporados al fichero serán los aportados por las entidades usuarias o participantes relativos a las solicitudes de operaciones recibidas. Tales datos se aportarán en el mismo momento en que se consulte la información sobre la posible detección de datos irregulares. Según el artículo 6.1 del Reglamento, sólo será posible la aportación cuando la solicitud sea firme y todos los datos marcados como obligatorios estén cumplimentados, según los campos indicados en el artículo 16.

El fichero permite la detección de datos denominados “irregulares”, que son los que no coinciden con los datos de otras operaciones que ya figuraban en el fichero, atendiendo a las reglas o premisas marcadas por cada entidad usuaria a través de su coordinador, en los términos descritos en el apartado 9.5 de la Memoria.

A partir de tales datos irregulares, una solicitud de operación será examinada por la entidad usuaria que, en su caso, podrá calificar una solicitud como incongruente. El artículo 6.6 del Reglamento especifica que “En ningún caso la detección de datos irregulares en el FICHERO CONFIRMA será causa de denegación de la operación solicitada, que quedará supeditada al resultado del examen a que se refiere el párrafo anterior”; lo que reitera el apartado 9.6 de la Memoria.

3.- La suscripción del Reglamento supone, de conformidad con el art. 2, el compromiso por parte de las Entidades usuarias o participantes del cumplimiento de sus normas. Se configura así en el Capítulo Quinto un sistema de control de cumplimiento a través de la Comisión de Control, compuesta por representantes de los responsables del fichero y del encargado del tratamiento; se disciplinan normas sobre el sistema de

nombramiento de estos representantes, sus competencias y funciones, y se instaura un régimen sancionador.

4.- Los responsables del fichero son, según el artículo 3, las entidades adheridas al sistema “que tienen el interés legítimo de luchar y prevenir el fraude en solicitudes de operaciones”; por ello, el artículo 4 configura como requisito imprescindible para la participación en el Fichero que la entidad pueda ser objeto de fraude en la contratación en su ámbito de actividad, realizando operaciones de financiación o de pago aplazado. Cada una de estas entidades contará con un Consultor del Fichero Confirma. El artículo 8.1 del Reglamento especifica sus obligaciones y responsabilidades.

5.- CONFIRMA SISTEMAS DE INFORMACIÓN, S.L. será el encargado del tratamiento del fichero en cuestión, afirmándose que existen los correspondientes contratos de encargo de tratamiento en los términos del art. 12 LOPD, cuyos aspectos más importantes se detallan en el apartado 6 de la Memoria.

(...)

7.- El Reglamento afirma partir del sometimiento a la normativa sobre protección de datos personales, y en particular reitera el principio de mínimo acceso a la información, el cumplimiento del deber de información del art. 5 LOPD, la legitimación sin consentimiento del interesado con base en el interés legítimo, el sistema de ejercicio de los derechos de los interesados, así como la conservación de los datos por un periodo de un año, salvo en el caso de solicitudes calificadas como incongruentes y vinculadas, que será de dos años.

Las conclusiones de dicho informe fueron, en general, que el sistema se adecuaba a las exigencias de la normativa vigente en materia de protección de datos.

Asimismo, también se emitió el Informe 214/2016 de 21 de julio de 2016 referido a la adecuación a la normativa de protección de datos, de distintas modificaciones que se propusieron por la consultante, como la ampliación del ámbito de aplicación del Fichero Confirma para convertirlo en multisectorial en el que se estimó que se introducían las garantías adecuadas al criterio de esta Agencia recogido entre otros en el Informe 106/2014 de 7 de agosto de 2014:

(...) De este modo, ha considerado esta Agencia que el cruce de información referida a los distintos sectores podría implicar el acceso por entidades de un sector a información que habitualmente estas no

requieren para estimar o desestimar las solicitudes de servicio que se les formulan.

(...)para que un sistema como el descrito en la consulta pudiera resultar conforme a la Ley Orgánica 15/1999 sería necesario que el mismo no sólo aportase las garantías ya mencionadas en los ficheros de carácter sectorial que ya han sido informados por esta Agencia, sino que además debería aportar otra serie de garantías adicionales que impidieran que se produjese el efecto que esta Agencia ya ha advertido con anterioridad; es decir, el acceso a información adicional a la necesaria como consecuencia del intercambio de información sobre operaciones en sectores en que el fraude reviste, más allá de un mínimo común, una tipología enteramente diferenciada.

Estas garantías adicionales deberían, en primer lugar, referirse al conjunto de datos que podrían ser objeto de comparación para detectar como inconsistente una determinada operación, de modo que esos datos habrían de ser exclusivamente los que son comúnmente requeridos en los tres sectores a los que el sistema se refiere, sin que ningún otro dato requerido en uno o dos de los sectores pudiera generar ningún tipo de alerta ni, menos aún fuera revelado a las entidades participantes en caso de que la alerta se generase respecto a las informaciones.

De este modo, los datos objeto de comparación en este sistema deberán ser los mínimos comunes a los tres sectores involucrados, la información visualizada no podría exceder de la que lo sería para cada uno de los sectores y debería ir referida únicamente a las alertas generadas por inconsistencia en los datos que constituyen ese mínimo común y las reglas deberían fundamentarse única y exclusivamente en la inconsistencia en dichos datos, respetando siempre lo ya informado anteriormente por esta Agencia en el sentido de que cada entidad deberá poder configurar sus propias reglas pero siempre dentro del máximo que, para este fichero multisectorial se fijase por el responsable del fichero.”

También, en el citado informe 214/2016 se estimó conforme al principio de proporcionalidad (artículo 4 .1 de la LOPD, en la actualidad referido al principio de minimización previsto en el artículo 5.1 c) RGPD) la posibilidad de que el plazo de comprobación de los requisitos de la operación en casos de solicitudes de operación no presenciales se fijará en 45 días, para poder cotejar la documentación que las entidades concedentes de la operación reenvían a la entidad financiera concedente del crédito:

Ciertamente el plazo de 45 días puede considerarse prolongado a efectos de llevar a cabo la verificación. No obstante, la Memoria aportada justifica ese plazo en el hecho de que los establecimientos se demoran en la entrega de la documentación a contrastar. De este modo, si bien sería recomendable que en el futuro se adoptasen medidas tendentes a una reducción del plazo mencionado, podría informarse favorablemente la modificación establecida en este punto en las normas de funcionamiento del sistema.:

Y finalmente se abordó la posibilidad de que se indicará en el fichero la circunstancia de la existencia de múltiples solicitudes de financiación de un mismo producto, para evitar que el hecho de que un mismo consumidor haya realizado en un plazo reducido de tiempo diferentes solicitudes de financiación para el mismo tipo de producto en varias entidades a fin de conocer cuál de ellas le resultaría más ventajosa pueda ser considerado por sí mismo un indicio de la irregularidad de la operación, dado que esa práctica puede resultar habitual sin que por ello se produzca una situación de fraude. En el que se informó favorablemente por cuanto:

(...) la opción planteada coadyuvaría a una mejor proporcionalidad y calidad de la información reduciendo la incidencia de los mencionados falsos positivos.

Por este motivo, se considera que la citada modificación supone una mejora en cuanto a las garantías de protección de datos establecidas en el sistema.

II

La primera de las cuestiones que plantea la consultante es la referida al rol que deben desempeñar las Entidades Adheridas al sistema y Confirma en relación con la regulación del vigente RGPD, teniendo en cuenta que ha desaparecido de la regulación la categoría de “responsable del fichero” y la existencia de una categoría específica para los supuestos de corresponsabilidad (artículo 26 del RGPD y artículo 29 de la LOPDGDD).

Sobre la posición jurídica de los intervinientes en el tratamiento de datos personales que se deriva de la participación en el Fichero Confirma la consulta plantea una posible modificación del reparto de roles que existía hasta ahora, dónde las entidades adheridas eran responsables del fichero y Confirma era encargada del tratamiento de aquellas.

Con carácter previo al análisis del rol que deben desempeñar los intervinientes en el tratamiento de datos que se deriva de la participación en el Fichero Confirma, y teniendo en cuenta la terminología utilizada hasta ahora, sobre el

uso del concepto “responsable del fichero”, bajo el régimen del RGPD esta Agencia se ha pronunciado en el Informe 94/2022 en el que se aborda la redacción de un proyecto de una disposición de carácter general dónde se utiliza dicho término:

(...)conviene indicar que una de las novedades del RGPD, es que la noción de “fichero” ya no es uno de los elementos clave del sistema de protección de datos, ya no puede ser considerada como piedra angular del sistema, que venía a determinar por su mera existencia la aplicación de la normativa y otorgaba una posición relevante a determinados intervinientes en el tratamiento de datos como era el “responsable del fichero” y suponía el sometimiento al régimen sancionador previsto en la hoy derogada LOPD de 1999 (Artículo 43).

Ahora la regulación se centra principalmente en el “tratamiento” como eje fundamental en la normativa de protección de datos.

La pérdida de relevancia de dicho elemento, la encontramos, por ejemplo, en el Capítulo IV del RGPD, bajo la denominación “Responsable del tratamiento y encargado del tratamiento” únicamente se regulan estas figuras junto con los supuestos de corresponsabilidad. Es decir, ha desaparecido la figura del responsable del fichero, como tampoco aparece en las definiciones del artículo 4 como si lo hace el responsable y el encargado.

Asimismo, otra muestra de la pérdida de relevancia del fichero como elemento en protección de datos, se observa con la desaparición de la obligación de inscribir el fichero en el extinto Registro General de Ficheros de la AEPD que ha sido suprimida de la actual normativa, pudiendo entenderse sustituido por la obligación de disponer de un Registro de Actividades del Tratamiento, en los supuestos previstos en el artículo 30 del RGPD y artículo 31 de la LOPDGDD.

En la actualidad, la noción de fichero la encontramos en el RGPD, únicamente, en el apartado de definiciones (artículo 4.6) y como elemento de aplicación material del reglamento, cuando estemos ante el tratamiento no automatizado de datos personales que estén “contenidos o destinados a ser incluidos en un fichero” (artículo 2.1).

Es decir, resulta obvio la aplicación residual del concepto del fichero en la vigente normativa de protección de datos, en comparación con el régimen jurídico que se derivaba de la Directiva 95/46/CE.

En consecuencia, la redacción del precepto en lo que se refiere a este aspecto ha de considerarse obsoleta pues parece obedecer a la anterior

regulación, al indicar “fichero titularidad de (...)”, a pesar de no hacerlo expresamente, está utilizando implícitamente el concepto de “responsable del fichero” que hoy en día no consta ni en el RGPD ni en la LOPDGDD. Por lo que se propone su eliminación.

(...)

Teniendo en cuenta lo anterior, se propone a la consultante que resultaría más adecuado a la terminología utilizada en la actualidad en el marco jurídico de protección de datos, la sustitución de la denominación “Fichero Confirma” por Sistema Confirma (o la que la consultante estime más adecuada), y la supresión de la figura de Responsable del fichero en tanto no tiene encaje normativo en la actualidad y puede inducir a error o confusión y se sustituya por la categoría que, en su caso, proceda y que es objeto de análisis a continuación.

En efecto, para la correcta aplicación de la normativa sobre protección de datos personales se 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.

Sin perjuicio de la atribución de obligaciones directas al encargado, que se citan en el apartado IV del presente informe, 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.

Por otro lado, debe abordarse también la figura del corresponsable del tratamiento, o supuestos de corresponsabilidad que el artículo 26 del RGPD prevé:

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

51. “En términos generales, existe una corresponsabilidad del tratamiento concreta cuando diferentes partes determinan conjuntamente los objetivos y los medios del tratamiento”

Y partiendo igualmente de que 52. “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”.

54. La corresponsabilidad puede resultar de decisiones convergentes de dos o más entidades en relación con los fines y medios esenciales. (...) un criterio importante para identificar decisiones convergentes en este contexto es si el tratamiento no sería posible sin la participación de ambas partes en los fines y medios en el sentido de que el tratamiento por cada parte es inseparable, es decir, inextricablemente vinculado.

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).

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, la consulta procede a revisar la asignación de roles que se validó en el

Informe 150/2013, para adecuarla a la normativa actual sobre protección de datos personales.

III

Son varios los elementos que han de ser abordados para la determinación del rol de los intervinientes en el tratamiento de datos derivado del Fichero Confirma, como por ejemplo el aspecto funcional en relación con el tratamiento, la finalidad perseguida, la base jurídica que legitima el tratamiento y las obligaciones asumidas por los distintos actores.

Con carácter previo hay que recordar que la finalidad del tratamiento de los datos en el Fichero Confirma es la prevención del fraude y es un requisito de adhesión que la entidad usuaria del sistema “En su ámbito de actividad pueda ser objeto de fraude en la contratación, realice operaciones de financiación o de pago aplazado” (artículo 4 de su Reglamento)

Por lo tanto, la finalidad del tratamiento y los requisitos objetivos de participar en dicho tratamiento están perfectamente delimitados, y serán un denominador común en los participantes en el sistema.

La primera cuestión que se debe tener en cuenta es la base jurídica que legitima el tratamiento de datos personales en el Fichero Confirma, siendo el interés legítimo la que se impone de forma más evidente respecto de las restantes previstas en el artículo 6.1 del RGPD.

En efecto, el interés legítimo como base jurídica para la lucha y prevención del fraude resulta, con carácter general, la más adecuada (salvo otros sectores regulados como por ejemplo el asegurador el cual dimana de la obligación legal ex artículo 100 de la LOSSEAR), y se cita expresamente en el Considerando 47 del RGPD al indicar que:

El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate.

Así como en el propio Dictamen 6/2014 del Grupo de Trabajo del Artículo 29 referido al artículo 7 f) de la Directiva 95/46, que puede tomarse en consideración a la hora de interpretar la aplicación del artículo 6.1 f) del RGPD:

La prevención del fraude —que puede comprender, entre otros, la supervisión y la elaboración de perfiles de clientes— es otro ámbito típico que es probable se considere que excede de lo que se estima necesario para la ejecución de un contrato. Dicho tratamiento podría ser en tal caso legítimo en virtud de otro fundamento jurídico del artículo 7, por ejemplo, (...) el interés legítimo del responsable del tratamiento

(artículo 7, letras a), c) y f)). En este último caso, el tratamiento deberá quedar sujeto a garantías y medidas adicionales para proteger adecuadamente los intereses o los derechos y libertades de los interesados. (...)

La siguiente es una lista no exhaustiva de algunos de los contextos más comunes en los que puede surgir la cuestión del interés legítimo en el sentido del artículo 7, letra f). Se presenta a continuación sin perjuicio de si los intereses del responsable del tratamiento prevalecerán en último término sobre los intereses y los derechos de los interesados cuando se realice la prueba de sopesamiento.

- la prevención del fraude, el uso indebido de servicios o el blanqueo de dinero;

Y también en el citado Dictamen se pone un Ejemplo estrechamente relacionado con una de las funcionalidades del Fichero Confirma como es la verificación de irregularidades en la identidad de los solicitantes de operaciones de crédito:

Ejemplo 10: Verificación de los datos de los clientes antes de la apertura de una cuenta bancaria

Una institución financiera sigue procedimientos razonables y proporcionados (...) para verificar la identidad de cualquier persona que desee abrir una cuenta. Mantiene registros de la información utilizada para verificar la identidad de la persona.

El interés del responsable del tratamiento es legítimo, el tratamiento de datos afecta únicamente a información limitada y necesaria (práctica normalizada en la industria, que los interesados pueden esperar razonablemente, y recomendada por las autoridades competentes). Se prevén las garantías adecuadas para limitar cualquier impacto desproporcionado e indebido sobre los interesados. Por tanto, el responsable del tratamiento puede utilizar el artículo 7, letra f), como fundamento jurídico.

De este modo, y sin perjuicio del jurídico de ponderación o prueba de sopesamiento y la adopción de garantías suficientes, la base jurídica del tratamiento será la prevista en el artículo 6.1 f) del RGPD referida a cuando el tratamiento es necesario para satisfacer el interés legítimo del responsable o de un tercero.

Teniendo en cuenta lo anterior, las entidades usuarias son las que tienen ese interés legítimo en protegerse del fraude a través de su participación en el

Fichero Confirma. Interés y finalidad que son distintos de los que puede perseguir la propia entidad consultante, proveedora de la plataforma tecnológica.

Por tanto, estas entidades persiguen la misma finalidad y han de cumplir los mismos requisitos. Estos elementos también deben ser tenidos en cuenta a la hora de delimitar que rol tendrán estas y otras entidades en relación con el tratamiento de datos personales. (responsable del tratamiento, encargado y corresponsables).

Dicho esto, es preciso recordar el funcionamiento del Fichero Confirma, que, en síntesis, consiste en que cada entidad usuaria realiza una consulta al sistema aportando determinada información sobre una solicitud de operación que le hayan hecho y ésta es contrastada con otras solicitudes de información que ya estén incorporadas al sistema con la finalidad de buscar coincidencias o irregularidades que, según unos criterios predefinidos, haga que el sistema califique dichas solicitudes como “irregulares” o como “vinculadas” según los casos.

Es decir, el funcionamiento del sistema se nutre de datos facilitados por las entidades que reciben las solicitudes de operaciones para su posterior cotejo entre sí.

De este modo para que el sistema cumpla su finalidad es necesario la participación de cada entidad usuaria, pues de otro modo no tendría sentido que una sola entidad utilizara este sistema, ya que podría hacer esa comparación de sus propias solicitudes y de sus propios clientes en sus propios sistemas sin necesidad de utilizar el Fichero Confirma cuyo valor añadido es, precisamente, la comparación de solicitudes con terceros. (lo que no obsta a que el sistema para un funcionamiento más completo también permita a las entidades usuarias comparar las solicitudes con las de su misma entidad, pero ese no es el valor añadido que ofrece el sistema).

Esta circunstancia, referida a la necesidad de participación en el sistema de otras entidades, tal como se explica más adelante resulta determinante a la hora de establecer el rol de interviniente en el tratamiento de datos.

Cada entidad usuaria es responsable del tratamiento, ya que determina los medios y los propósitos del mismo. (artículo 4.7 RGPD). Dicho de otro modo, éstas determinan “el qué” va a someterse a tratamiento (la solicitudes de operaciones que recibe, obviamente con datos personales) y el “para qué” del tratamiento (para su comparación con el fin de detectar irregularidades y prevenir el fraude).

Dicho lo anterior, debe indicarse que estamos ante un supuesto de corresponsabilidad a la que se refiere el artículo 26 del RGPD antes transcrito, y respecto del que las Directrices 07/2020 del CEPD indican lo siguiente:

54. La corresponsabilidad puede resultar de decisiones convergentes de dos o más entidades en relación con los fines y medios esenciales. (...) un criterio importante para identificar decisiones convergentes en este contexto es si el tratamiento no sería posible sin la participación de ambas partes en los fines y medios en el sentido de que el tratamiento por cada parte es inseparable, es decir, inextricablemente vinculado.

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.

En efecto, en el presente caso la finalidad del tratamiento no podría cumplirse sin la participación de los distintos responsables del tratamiento, ya que, como se ha indicado antes, la participación unilateral en el sistema no tendría sentido ni sería efectiva en la lucha contra el fraude en términos cuantitativos ni cualitativos.

Asimismo, según el Reglamento del Fichero Confirma, cada entidad usuaria responde de la veracidad y exactitud de la información aportada y asumen cualquier responsabilidad que pudiera derivarse de esa información, comprometiéndose a *“aportar/consultar, rectificar y cancelar la información conforme a la normativa de protección de datos de carácter personal”* (artículo 6.2 y 3 de su Reglamento).

En este sentido debe indicarse que estas obligaciones, también se asumen, frente a las otras entidades, lo que refuerza aún más la consideración de corresponsables del tratamiento por cuanto el cumplimiento de las mismas, por cada entidad, es condición sine qua non para que el sistema funcione correctamente y se cumpla la finalidad pretendida.

Es, por tanto, necesaria la colaboración entre todas ellas para el adecuado funcionamiento del Fichero Confirma, determinando de este modo conjuntamente los medios, y la finalidad del tratamiento. Y también respondiendo de la veracidad y exactitud de la información aportada.

Por lo tanto, la relación entre las entidades usuarias del sistema se articula como un supuesto de corresponsabilidad previsto en el artículo 26 del RGPD.

En el que, como a continuación se explica, no cabe la entidad Confirma por cuanto ni realiza un tratamiento de datos similar, ni debe cumplir ciertos

requisitos, ni tampoco asume aquellas obligaciones, sino que es un proveedor de la infraestructura, y no persigue un fin propio como las citadas entidades usuarias. (las Directrices 7/2020 en el apartado 68 considera que la existencia de un mero beneficio comercial para las partes involucradas no es suficiente para que se considere fin del tratamiento).

Asimismo, tampoco puede atribuírsele que persigue la misma finalidad o que su “interés legítimo” es el mismo interés que el de las entidades usuarias. En este sentido en el Informe 81/2019 sobre los sistemas de información de cumplimiento de obligaciones dinerarias o ficheros positivos, se indicaba lo siguiente:

“existiría una confusión entre la finalidad del tratamiento y el interés legítimo, ya que como recuerda el Dictamen 6/2014, “El concepto de «interés» está estrechamente relacionado con el concepto de «finalidad» mencionado en el artículo 6 de la Directiva, aunque se trata de conceptos diferentes. En términos de protección de datos, «finalidad» es la razón específica por la que se tratan los datos: el objetivo o la intención del tratamiento de los datos. Un interés, por otro lado, se refiere a una mayor implicación que el responsable del tratamiento pueda tener en el tratamiento, o al beneficio que el responsable del tratamiento obtenga —o que la sociedad pueda obtener— del tratamiento”.

Por otro lado, el interés legítimo se centraría en el de las terceras entidades concedentes de crédito, dirigido a cumplir con sus obligaciones de evaluación de la solvencia y también en su interés económico, derivado de un mayor conocimiento de sus clientes y la disminución del riesgo de las operaciones de crédito. Sin embargo, no se cita en ningún momento el interés legítimo propio del responsable, que sería el de obtener un beneficio económico, interés legítimo, sin duda, pero que no significa que prevalezca sobre la protección de datos de las personas, habiendo sentando nuestro Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección Tercera), como doctrina de interés casacional, en la Sentencia núm. 815/2020, de 18 de junio (reiterada en las número 839/2020, 840/2020 y 853/2020, todas de 22 de junio de 2020) que “los intereses comerciales de una empresa responsable de un fichero de datos han de ceder ante el interés legítimo del titular de los datos en la protección de los mismos”.

En conclusión, la entidad Confirma, con un marcado interés económico o comercial, no puede considerarse que persigue la misma finalidad que las entidades usuarias, como tampoco puede atribuírsele la misma base jurídica

que legitimaría el tratamiento por parte de aquellas, por cuanto los elementos a tener en cuenta en un hipotético juicio de ponderación o prueba de sopesamiento son distintos y en consecuencia, el resultado de dicha ponderación puede que sea favorable a la prevalencia de los intereses de los afectados.

IV

En cuanto a la entidad Confirma, en el Informe 150/2013 de fecha 30 de abril de 2013, sobre la adecuación del Reglamento del Fichero Confirma a la normativa de protección de datos personales, se consideró como encargado del tratamiento de las entidades usuarias del sistema por cuanto se informó favorablemente, y así ha seguido considerándose formal y materialmente hasta ahora en la práctica habitual derivada del funcionamiento del Fichero Confirma.

En la actualidad debe confirmarse tal consideración por cuanto el marco jurídico actual no ha modificado sustancialmente los criterios a tener en cuenta para considerar que estamos ante un encargado del tratamiento (así se indica expresamente en el apartado 11 de las citadas Directrices 7/2020), sino que, entre otras cuestiones, ha concretado y delimitado las obligaciones de esta figura.

Por lo que sí, fáctica y funcionalmente, la posición de Confirma no ha sufrido cambios significativos respecto de los elementos que se tuvieron en cuenta en el Informe 150/2013, **la solución más coherente y respetuosa con la seguridad jurídica, es considerar que seguimos estando ante un encargado del tratamiento, con las obligaciones inherentes a tal condición que se derivan del actual marco jurídico.**

En este sentido, partiendo del principio de responsabilidad proactiva, dirigido esencialmente al responsable del tratamiento, y al objeto de reforzar la protección de los afectados, debe recordarse que 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 citadas Directrices 07/2020 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.

Por lo tanto, **Confirma ha de considerarse encargada del tratamiento de las otras entidades usuarias corresponsables del tratamiento**, debiendo cumplir las obligaciones que se acaban de indicar, y en especial, en referencia a lo planteado en la consulta, debe suscribir un contrato de encargado del tratamiento en los términos del artículo 28.3 del RGPD con cada entidad usuaria del sistema.

V

En otro orden de cosas, la consultante plantea la posibilidad de ampliar el plazo de conservación de las solicitudes en el Fichero Confirma.

En la actualidad hay que atender a los tipos de solicitudes que prevé el Reglamento del Fichero Confirma, en primer lugar la “solicitud incongruente” que es aquella solicitud de operación en la que se haya detectado datos irregulares y que ha sido calificada como “incongruente” por el coordinador de la entidad después de la revisión, estudio e investigación de la solicitud de operación y en segundo lugar la denominada “solicitud de operación vinculada” que son aquellas que sin haber sido calificadas como incongruentes, han provocado la detección de datos irregulares en otras solicitudes de operación. Ambas tienen un plazo de conservación en el sistema de dos años.

Asimismo, la consultante manifiesta que el plazo general de conservación de solicitudes (no determina cuales) es de un año, y de dos años para las antes referenciadas: solicitud incongruente y solicitud vinculada.

En el mismo sentido el Artículo 18 del Reglamento del Fichero Confirma bajo la denominación “Permanencia de los datos en el Fichero Confirma” dispone lo siguiente:

Los datos contenidos en el Fichero Confirma que no sean cancelados por las ENTIDADES USUARIAS O PARTICIPANTES, serán cancelados por CONFIRMA SISTEMAS DE INFORMACIÓN, S.L., por cuenta del RESPONSABLE del FICHERO, una vez transcurridos los periodos de permanencia, fijados en dos años para las SOLICITUDES

INCONGRUENTES y SOLICITUDES DE OPERACIONES VINCULADAS y un año para el resto de SOLICITUDES.

En cuanto a la justificación de los referidos plazos de permanencia en el SISTEMA, en la Memoria del Reglamento del Fichero CONFIRMA aportada a la consulta a raíz de la cual se emitió el Informe 150/2013, en el apartado 9.15 se hace constar lo siguiente:

Los datos relativos a solicitudes de operaciones permanecerán en el Fichero Confirma dos años en el caso de solicitudes incongruentes y solicitudes vinculadas y un año en el resto de las solicitudes.

La fijación de los plazos anteriores tiene su base en el interés legítimo de las Entidades participantes en la prevención del fraude, que necesitan almacenar datos durante un periodo de tiempo suficientemente largo como para que puedan cruzarse con nuevas solicitudes. Al mismo tiempo, los datos tienen que ser lo suficientemente recientes como para proporcionar un beneficio al identificar las solicitudes fraudulentas sin detectar falsas irregularidades, derivadas de la modificación de los datos por el transcurso del tiempo (cambio de dirección, de trabajo, etc.).

Si bien la premisa anterior marca los límites teóricos de mantenimiento de los datos, para la determinación de los plazos concretos se han tenido en cuenta los distintos tipos de fraude en solicitudes detectados en las entidades con las que se ha mantenido entrevistas, así como los tiempos de detección del mismo que, a través de la documentación analizada, se ha comprobado que son coincidentes en otros países de la Unión Europea:

- * El 29% de los casos de fraude se detecta antes del transcurso de 6 meses desde la concesión de la operación.*
- * El 20% entre los 6 y 12 meses.*
- * El 25% entre los 12 y 24 meses.*
- * El 14% entre los 2 y 3 años.*
- * El 5% entre los 3 y 4 años.*
- * El 3% entre los 4 y 5 años.*
- * El 4% se detecta después de 5 años.*

La determinación del plazo genérico de un año para el mantenimiento de los datos y de dos años para aquellas operaciones incongruentes o vinculadas da respuesta a la mayor parte de los casos de fraude (las $\frac{3}{4}$

partes) y cubre la duración máxima de los fraudes organizados, cuya duración se fija en aproximadamente 12 meses”.

Teniendo en cuenta esta explicación, en el Informe 150/2013 se estimó adecuados los plazos de conservación propuestos al indicar que:

(...) En cuanto a la conservación de los datos, que como hemos adelantado permanecerán en el Fichero Confirma dos años en el caso de solicitudes incongruentes y solicitudes vinculadas y un año en el caso del resto de solicitudes, aparece suficientemente justificada tras un estudio sobre las necesidades de conservación de estos datos en relación con la finalidad perseguida de prevención del fraude. (...)

Pues bien, ahora se pretende la modificar los plazos de la siguiente manera, el plazo general de un año ampliarlo a tres años, y el plazo de las solicitudes incongruentes y de las solicitudes vinculadas de dos años ampliarlo a cinco años, y se plantea si esta modificación seria conforme a los principios de limitación del plazo de conservación y de exactitud.

Sobre los citados principios, el artículo 5 apartado 1 letras d) y e) del RGPD, dispone lo siguiente:

Los datos personales serán:

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

Respecto del principio de exactitud, a priori, no se considera que pueda verse afectado gravemente, por cuanto los criterios o parámetros para la calificación de las operaciones como incongruentes o como vinculadas, se regulan por las entidades usuarias sobre las posibilidades que ofrece la plataforma tecnológica. Así se establece en el apartado 9.5 de la Memoria del Reglamento del Fichero CONFIRMA.

De tal modo que el plazo durante el que se mantienen unos datos conforme a esas “reglas” no modifica la realidad que deben ostentar esos datos pues en puridad, el plazo no cambia dichas reglas, que son las que hacen que unos datos personales (una solicitud de operación registrada en el fichero) tengan un significado y otro.

Es decir, no estamos ante otro tipo de sistemas de información, como los de información crediticia previstos en el artículo 20 de la LOPDGDD, en los que el mero hecho de que unos datos consten allí significa, salvo prueba en contrario, que existe una deuda, cierta, vencida y exigible y que ha sido requerida de pago. Dónde el elemento temporal juega un papel determinante en relación con el principio de exactitud, por cuanto mientras los datos se encuentren incluidos en estos sistemas de información crediticia, supone per se, que el titular de los mismos es deudor, y frente a los que puede ejercer su derecho de supresión por entender que no se cumplen los requisitos indicados, y que por tanto no debe considerarse deudor y en consecuencia sus datos no reflejan el testimonio de la realidad que deben tener.

Sin embargo, en el Fichero CONFIRMA lo que se pone de manifiesto es la incongruencia o irregularidades en las solicitudes de operaciones conforme unos parámetros previamente definidos, por lo que el plazo durante el tiempo en el que estén no afecta gravemente a la existencia o no de dichas incongruencias o irregularidades. Tanto es así, que no podría explicarse de modo lógico y razonable, por qué razón un plazo de dos años no vulneraría ese principio de exactitud y otro de cinco años si lo pudiera vulnerar. Es decir, esto responde a la reglas previamente fijadas por las entidades.

A los principios que puede afectar una modificación del plazo de constancia de determinadas solicitudes, sería al de conservación y al de finalidad, que se abordan posteriormente.

En consecuencia, la modificación de los plazos propuestas no se entiende que vulnera el principio de exactitud de los datos. Sin perjuicio de que, obviamente, el titular de los datos mantiene incólume el ejercicio de los derechos previstos en los artículos 15 a 22 del RGPD, y en especial el de rectificación, especialmente vinculado con el principio de exactitud, y el responsable su obligación de tratar los datos conforme a dicho principio.

Respecto al principio de limitación del plazo de conservación, éste se encuentra estrechamente vinculado al principio de minimización (y en última instancia al de limitación de la finalidad), es decir, es la “manifestación temporal del principio de minimización”, te tal modo que los datos no pueden tratarse más allá del tiempo estrictamente necesario para alcanzar la finalidad que

persigue el tratamiento en cuestión. En este sentido, nos recuerda el Considerando 39 del RGPD que:

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

Para analizar la adecuación a la “necesidad del tiempo de tratamiento” para cumplir la finalidad perseguida, y que supone una modificación de los plazos de conservación de los datos en el Fichero CONFIRMA la consultante indica lo siguiente:

Tras años de funcionamiento del Fichero se detecta la necesidad de ampliar la permanencia de los datos en el Fichero Confirma en atención a un doble motivo:

- Contar con información suficiente de solicitudes incongruentes, lo que permitiría contrastar los datos de nuevas solicitudes y detectar las posibles irregularidades. Aumentar este plazo de permanencia permite lidiar de una manera más eficaz contra los supuestos de fraude durmiente y reiterado.*
- Contar con información de solicitudes previas que no han sido declaradas incongruentes, lo cual permite realizar reglas de congruencia y buscar coincidencias de datos con solicitudes anteriores, con el objeto de reducir la posibilidad de fraude por suplantación de identidad.*

(...) para valorar la idoneidad de estos plazos, tras el análisis realizado por Confirma se alcanzan las siguientes conclusiones sobre la frecuencia de variación de los datos tratados en el Fichero en atención a cada tipología:

- En el caso del domicilio, como consecuencia del análisis del funcionamiento del Fichero Confirma, con ayuda de las Entidades Adheridas al Fichero se ha verificado que las comunicaciones de cambio de domicilio de sus clientes no suelen tener lugar en plazos inferiores a los tres o cuatro años. Asimismo, la propia Ley 19/1994, de 24 de noviembre, de Arrendamientos Urbanos, aunque prevé que la duración será libremente pactada por las partes, sí que contempla un plazo de tres a cinco años como duración más habitual para este tipo de contratos.*

•Con relación a los cambios laborales, según las estadísticas de frecuencia de cambio de puestos de trabajo, se observa que, en promedio, el periodo mínimo de permanencia en un puesto de trabajo en España suele oscilar entre uno y tres años.

Teniendo en cuenta lo anterior, el plazo general de conservación de un año previsto inicialmente en el Fichero Confirma se estima demasiado corto para poder dar cumplimiento a la finalidad del Fichero. En consecuencia, la ampliación a un plazo general a tres años resulta más adecuada para lograr la finalidad perseguida, sin que se vea afectada la exactitud de los datos en el Fichero.

Con relación al plazo de dos años previsto inicialmente para las solicitudes calificadas como "incongruentes" o "no concluyentes", se plantea su ampliación a cinco años de permanencia en el Fichero Confirma.

La ampliación de los plazos de permanencia de los datos en el Fichero Confirma tiene impacto en el cumplimiento del principio de limitación del plazo de conservación y en el principio de exactitud. En este sentido, los nuevos plazos de conservación se han definido en atención al análisis e investigación del sector y del funcionamiento del propio Fichero llevados a cabo, concluyéndose que los mismos se estiman adecuados en atención a la finalidad del tratamiento.

Teniendo en cuenta lo manifestado por la consultante, y sin perjuicio de que esta Agencia no tiene la absoluta certeza del origen y veracidad de los parámetros citados referidos a los cambios de domicilio y de puesto de trabajo, que, entre otras circunstancias y según la consultante, hacen necesarios la modificación propuesta, a priori, parece que dicha ampliación está suficientemente justificada tras el estudio realizado sobre las necesidades de conservación en relación con la finalidad perseguida de prevención del fraude.

VI

Asimismo, la consultante propone la creación de otros dos "estados" en las consultas de operaciones en el Fichero CONFIRMA, uno denominada "posible suplantación de identidad" y otro denominado "en revisión".

Respecto del primero, la consultante sostiene que las suplantaciones de identidad suponen el 64 % de los casos identificados como fraude, lo que hace necesario una mejora en la detección, por lo que *la creación de ese nuevo estado permitiría una gestión diferenciada al margen de la categoría genérica de solicitud incongruente. La solicitud que se marcara con este nuevo estado tiene como consecuencia que la entidad consultante deberá comprobar más rigurosamente la identidad del solicitante, de cara a que no se trata de un*

nuevo intento de suplantación. En cuanto al plazo de conservación, se indica que será de cinco años.

La consultante plantea si la creación de este nuevo estado tiene implicaciones en el principio de licitud, y en concreto en la legitimación del tratamiento en el cumplimiento del interés legítimo.

Pues bien, como se ha indicado en el apartado III del presente informe, la base jurídica que legitima el tratamiento en este sistema de prevención y lucha contra el fraude, es efectivamente, la prevista en el artículo 6.1 f) del RGPD, sin que se estime que la creación de un nuevo estado afecte al mismo.

Lo que no obsta a que el responsable del tratamiento, previa prueba de sopesamiento o juicio de ponderación, establezca la prevalencia de su interés y las garantías suficientes para compensar o aminorar la posible injerencia que podría suponer añadir esta nueva categoría.

En consecuencia, y con las salvedades que se acaban de indicar, la creación de este nuevo estado “posible suplantación de identidad” resulta conforme los principios de licitud y limitación del plazo de conservación.

Respecto del segundo, la creación de un estado temporal de “en revisión”, la consultante sostiene que serviría a la detección de irregularidades en el comportamiento tras la concesión de la solicitud, ya que se ha detectado que las suplantaciones de identidad, en un primer estadio, son confundidas con retrasos en el pago y solo se descubre el fraude pasado un plazo desde la concesión. Con la creación de esta nuevo estado “en revisión” las entidades adheridas que reciban nuevas solicitudes y que se vinculen con otras “en revisión” podrán realizar respecto de aquellas, las comprobaciones tendentes a confirmar la identidad del solicitante desde el inicio.

Para el uso de este nuevo estado temporal, la consultante indica que se han de cumplir los siguientes requisitos:

- I. Que las irregularidades se produzcan por parte del interesado tras la concesión de la operación y
- II. que resulte imposible localizar a dicho titular.
- III. Únicamente se puede utilizar esta situación durante los seis meses posteriores a la concesión de la operación.

La consultante plantea si la creación de este nuevo estado tiene implicaciones en el principio de limitación de la finalidad y en el de minimización.

Sobre los citados principios, el artículo 5 apartado 1 letras b) y c) del RGPD dispone lo siguiente:

Los datos personales serán:

- b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (...) («limitación de la finalidad»);
- c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

Por su parte, el Considerando 39 indica que

los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.

Y el Considerando 50 indica que

El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales.

Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. (...). En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición.

Teniendo en cuenta lo señalado por la consultante, la finalidad que persigue este nuevo estadio “en revisión” es la lucha y prevención del fraude, que no sólo ha de valorarse antes de la concesión, sino que también puede aportar un valor añadido y perfeccionar el sistema, teniendo en cuenta irregularidades producidas en otras operaciones en los primeros meses tras su concesión y que sirva para detectar o identificar esas potenciales irregularidades en

solicitudes de operaciones que han recibido las entidades y que aún no han concedido.

Por lo que, sin perjuicio de que el conocimiento de la técnica, de las particularidades del sector y de las necesidades del sistema, corresponde a la consultante, desde el derecho a la protección de datos, esta Agencia considera que la finalidad a la que obedece la creación de este nuevo estadio “en revisión” está suficientemente justificada y no supone una quiebra del principio de limitación de finalidad y de minimización, por cuanto se adoptan garantías adecuadas para que su utilización no se convierta en injustificada y se aparte de la finalidad pretendida, como es la limitación a supuestos en los que ya ha sido concedida la operación, el titular se encuentre ilocalizable y durante un tiempo limitado tras la dicha concesión, esto es a 6 meses.

Es decir, se valora positivamente el establecimiento de requisitos para poder acceder al sistema de información en el supuesto examinado.

En este sentido esta Agencia ya se pronunció en el Informe 7/2015 sobre la necesidad de cumplir requisitos para el acceso a sistemas de información crediticia (previstos en el artículo 42.1 del RDLOPD) y que, por las similitudes con el supuesto analizado, conviene recordar:

*Por consiguiente, la mera adhesión al fichero de solvencia no puede ser considerada como una legitimación para el acceso indiscriminado a sus datos, **siendo necesario el previo cumplimiento** de los requisitos mencionados.*

VII

Por último, la consultante solicita el parecer de esta Agencia en relación con la posibilidad de que las entidades adheridas o usuarias al sistema, puedan consultar la congruencia o incongruencia de la información aportada por los interesados, no solo en el momento de solicitud de la contratación, sino también a lo largo de la vida de la operación en caso de resultar concedida.

Según la consultante *“Esto se justifica por la experiencia de los años de funcionamiento del Fichero Confirma, en los cuales se ha identificado que existen numerosos casos de fraude que se detectan tiempo después de que la operación se haya concedido”.*

La respuesta a de ser negativa por cuanto una posibilidad de consulta sin límite temporal supone una vigilancia sistemática de los afectados en el sistema sin aparente justificación.

Asimismo, quedaría sin efecto cualquier argumento que se ha dado y, en su caso, validado anteriormente sobre la ampliación de plazos de determinadas

solicitudes, o límites temporales de determinados estadios que se proponen para su creación. Es decir, no se explica como esta posibilidad de consulta permanente, coexistiría con los plazos de permanencia de las distintas solicitudes durante los distintos estadios.

Admitiendo esta última propuesta de la consultante se quiebran varios principios que hacen que el Fichero CONFIRMA resulte conforme a la normativa de protección de datos, por cuanto la base jurídica que legitima el tratamiento, esto es el interés pasaría de legítimo a ilimitado y sin contrapesos aparentes pues ampararía una monitorización permanente e injustificada, que debería ceder en el juicio de ponderación ante los intereses de los afectados (descritos con mayor amplitud que los del responsable del tratamiento); también el principio de finalidad resultaría afectado por cuanto el tratamiento (no olvidemos que dentro de la definición de tratamiento prevista en el artículo 4 del RGPD se encuentra el acceso o consulta) se produciría “por si acaso” hubiera fraude en el futuro -y la finalidad debe estar determinada ex ante del tratamiento; así como el principio de limitación del plazo de conservación de los datos, ya que no encontraríamos límite alguno salvo el de la vida del préstamo u operación.

En consecuencia, no se considera conforme a la normativa de protección de datos la posibilidad de consulta permanente por parte de las entidades adheridas al Fichero CONFIRMA.

VIII

Finalmente se hace preciso recordar que frente a las modificaciones propuestas y en relación a la base jurídica que legitima el tratamiento en el Fichero CONFIRMA, la relevancia del principio de transparencia y derecho de información (artículos 12 a 14 del RGPD) y el respeto al principio de limitación de finalidad y de minimización que operan como garantía y contrapeso a la injerencia en el derecho a la protección de datos que supone la inscripción de los datos personales en el Fichero CONFIRMA.

Por lo que corresponsables del tratamiento, y en su caso, encargado del tratamiento, deben velar por que los afectados dispongan de toda la información sobre el tratamiento de sus datos personales y los derechos que les asisten, tanto en el momento de la solicitud de una operación, es decir, como parte del contenido del artículo 13 del RGPD.

Por todo ello, se considera conveniente que se lleve a cabo una modificación del Reglamento del Fichero Confirma (informado favorablemente mediante el Informe 150/2013 de fecha 30 de abril de 2013, así como las sucesivas modificaciones mediante el Informe 214/2016 de 7 de agosto de 2014) para

incorporar las indicaciones realizadas en el presente informe con el fin de dotar de seguridad jurídica a entidades usuarias y a terceros y de garantías adecuadas a los tratamientos de datos personales que se lleven a cabo.