



I

La consulta solicita el parecer de esta Agencia en relación con el Reglamento del Repositorio del Servicio de Información de los Sujetos Obligados (en adelante Repositorio SISO) y su conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

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

1. Conforme al artículo 1 del Reglamento, el fichero se configura como un fichero común de intercambio de información circunscrito a las entidades que tengan la consideración de sujetos obligados de conformidad con lo previsto por la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, dividido en diferentes compartimentos independientes de información que agruparán a uno o varios sectores de actividad atendiendo a la tipología de los sujetos obligados y a las características de la operativa seguida por éstos. Según se indica:

- El fichero tiene su fundamento jurídico en el Artículo 33.2 de la Ley 10/2010.
- Contiene datos relativos a las operaciones a las que se refieren los artículos 18 y 19 de la Ley 10/2010 aportadas por los usuarios participantes en el sistema.
- La información se aportará en relación con estas operaciones cuando de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla.
- Las operaciones incluidas en el fichero habrán sido efectivamente comunicadas al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

2. El responsable del fichero será la entidad consultante, encomendando el mantenimiento del repositorio a otra entidad con la que habrá firmado una contrato que reúna las características del artículo 12 de la Ley Orgánica 15/1999 y sus disposiciones reglamentarias de desarrollo, siendo usuarios del

fichero los sujetos obligados por la Ley 10/2010 y generándose compartimentos separados por categorías de sujetos obligados, de forma que aquéllos únicamente accederán a la información contenida en su correspondiente compartimento.

3. Además, el acceso se reserva a los órganos de control interno de los sujetos obligados, creados de conformidad con lo impuesto por el artículo 26 de la Ley 10/2010, debiendo los sujetos designar un coordinador que les represente ante el propio fichero. Al propio tiempo, se establece un régimen de responsabilidad en cuya virtud serán las entidades usuarias quienes hayan de responder de la exactitud y veracidad de la información incluida en el repositorio, imponiéndose a las mismas la obligación de garantizar que el fichero permanezca exacto y actualizado. En particular, se prevé que en caso de que el Servicio Ejecutivo procediera a la devolución de la operación comunicada de conformidad con lo establecido en la Ley 10/2010 deberá procederse a la cancelación del dato en el mismo día hábil o en el inmediato posterior a aquél en que la devolución hubiera tenido lugar.

4. El personal de los usuario que no formase parte de los órganos de prevención “exclusivamente podrán llevar a cabo consultas a su compartimento del REPOSITORIO SISO con el fin de recibir alertas o avisos sobre operaciones solicitadas o contratadas, en cumplimiento de las obligaciones de diligencia debida e información establecidas en la Ley 10/2010. Las citadas alertas o avisos en ningún caso contendrán datos relativos a las operaciones contenidas en el REPOSITORIO SISO, sino que consistirán en mensajes que adviertan a los empleados de los USUARIOS sobre la necesidad de llevar a cabo un estudio o examen especial sobre la operación solicitada”. En todo caso, el resultado de la consulta no determina la denegación de la operación solicitada, sino que dicha operación quedará supeditada al resultado del examen especial previsto en la legislación de prevención del blanqueo de capitales.

5. Se prevé en las normas de funcionamiento que , de conformidad con lo establecido en la Ley 10/2010 no serán de aplicación las normas contenidas en la Ley Orgánica 15/1999 en lo que respecta al deber de información al afectado y la estimación de sus solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, si bien se establece un modelo normalizado de contestación a las solicitudes de ejercicio, que será respondido incluso cuando la petición no reuniese la totalidad de los requisitos establecidos en la normativa de protección de datos, en que se indicará que, de conformidad con el artículo 33 de la Ley 10/2010, “no resulta de aplicación a dicho Repositorio lo dispuesto en la LOPD referente al ejercicio de los derechos de acceso, rectificación, cancelación y oposición”, añadiendo que “por los motivos expuestos hemos de desestimar su solicitud, si bien le informamos que le asiste el derecho a recabar la tutela de la Agencia Española de Protección de Datos conforme a lo establecido en el artículo 18 de la LOPD”.

6. Se prevé igualmente la implantación en el fichero de las medidas de seguridad de nivel alto, de conformidad con lo dispuesto en el artículo 33.5 de la Ley 10/2010, exigiéndose de los usuarios la implantación de este nivel de



medidas así como un específico compromiso de confidencialidad en cuanto a la información obtenida.

7. Finalmente, se prevé la creación de una comisión de control para cada uno de los compartimentos del repositorio, en que serán representados la entidad responsable y las entidades usuarias de forma paritaria, estableciéndose un régimen sancionador para los supuestos de incumplimiento de lo estipulado en las reglas de funcionamiento sometidas a informe, pudiendo las sanciones implicar la suspensión de la utilización del fichero, en caso de las infracciones graves, o la baja en el fichero por tres años, en caso de las muy graves.

II

Descrito en estos términos el fichero objeto de regulación por las normas sometidas a informe, la primera cuestión que debe plantearse en relación con el mismo es la de si el tratamiento de los datos que en las normas se describen y su comunicación a las entidades participantes se encuentra amparada por lo dispuesto en la Ley Orgánica 15/1999.

En este sentido, y como punto de partida, debe traerse a colación lo ya indicado por esta Agencia en su informe de 2 de agosto de 2011, referido a la posible creación y mantenimiento de un “registro de agentes de alto riesgo” por parte de la Asociación X, constituyéndose el mismo sobre la base de lo dispuesto en el artículo 33.2 de la Ley 10/2010. De este modo, el citado informe razonaba sobre la cobertura legal para el tratamiento de los datos en este tipo de sistemas en los siguientes términos:

“El artículo 6.1 de la Ley Orgánica 15/1999 dispone que “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”.

A su vez, conforme al artículo 11.1 de la Ley Orgánica “Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”, si bien, el consentimiento no será necesario, conforme al artículo 11.2 a) en caso de que la cesión se encuentre amparada en una norma con rango de Ley.

EL artículo 33.2 de la Ley 10/2010, de 28 de abril, al que se refiere expresamente la consultante, dispone que “los sujetos obligados podrán intercambiar información relativa a las operaciones a las que se refieren los artículos 18 y 19 con la única finalidad de prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo cuando de las características u operativa del supuesto

concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquélla”.

El artículo 18.1, a su vez, delimita claramente las operaciones a las que se referirá el artículo 33.2 citado, al establecer que “Los sujetos obligados comunicarán, por iniciativa propia, al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (en adelante, el Servicio Ejecutivo de la Comisión) cualquier hecho u operación, incluso la mera tentativa, respecto al que, tras el examen especial a que se refiere el artículo precedente, exista indicio o certeza de que está relacionado con el blanqueo de capitales o la financiación del terrorismo”. Asimismo, se añade que “en particular, se comunicarán al Servicio Ejecutivo de la Comisión las operaciones que, en relación con las actividades señaladas en el artículo 1, muestren una falta de correspondencia ostensible con la naturaleza, volumen de actividad o antecedentes operativos de los clientes, siempre que en el examen especial previsto en el artículo precedente no se aprecie justificación económica, profesional o de negocio para la realización de las operaciones”.

A su vez, el artículo 19 de la Ley, al que también se remite el precepto, se limita a establecer el deber de abstención de ejecución de las operaciones comunicadas al Servicio Ejecutivo, no añadiendo con consecuencia aclaración alguna en cuanto a la tipología de las operaciones a las que se remite el artículo 33.2.

De los preceptos descritos se desprenden por tanto dos primeras consecuencias en relación con el contenido de las operaciones respecto de las que podrá producirse el intercambio de información:

- En primer lugar, deberá tratarse, en todo caso, de operaciones que hayan sido objeto de comunicación al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, al amparo de la obligación impuesta en el artículo 18.1 de la Ley 10/2020.*
- En segundo lugar, la comunicación únicamente podrá referirse, de entre las operaciones descritas anteriormente, a aquéllas respecto de las que pueda ser previsible el intento de comisión reiterada ante otro sujeto obligado, coincidiendo la operativa llevada a cabo por el presunto infractor en ambos casos.*
- En todo caso, el intercambio de información podrá llevarse a cabo entre sujetos obligados.*

Junto con tales limitaciones, el artículo 33 de la Ley 10/2010 establece algunas previsiones específicas que delimitan el régimen aplicable a



estos ficheros, introduciendo algunas de ellas, como la prevista en el apartado 4 de dicho precepto, limitaciones específicas a la difusión de la información en el ámbito de los sujetos obligados.

Así, en primer lugar, establece el citado apartado que “El acceso a los datos a los que se refiere este precepto deberá quedar limitado a los órganos de control interno previstos en el artículo 26, con inclusión de las unidades técnicas que constituyan los sujetos obligados”.

A tal efecto, el párrafo segundo del artículo 26.2 de la Ley establece que “Los sujetos obligados establecerán un órgano adecuado de control interno responsable de la aplicación de las políticas y procedimientos a que se refiere el apartado 1. El órgano de control interno, que contará, en su caso, con representación de las distintas áreas de negocio del sujeto obligado, se reunirá, levantando acta expresa de los acuerdos adoptados, con la periodicidad que se determine en el procedimiento de control interno. Reglamentariamente se podrán determinar las categorías de sujetos obligados para las que no resulte preceptiva la constitución de un órgano de control interno, siendo las funciones de éste ejercidas en tales supuestos por el representante ante el Servicio Ejecutivo de la Comisión”, añadiendo los apartados 2 y 3 del artículo que “para el ejercicio de sus funciones el representante ante el Servicio Ejecutivo de la Comisión y el órgano de control interno deberán contar con los recursos materiales, humanos y técnicos necesarios. Reglamentariamente se determinará para determinadas categorías de sujetos obligados la exigencia de constitución de unidades técnicas para el tratamiento y análisis de la información” y que “los órganos de prevención del blanqueo de capitales y la financiación del terrorismo operarán, en todo caso, con separación funcional del departamento o unidad de auditoría interna del sujeto obligado”.

Asimismo, se prevé en el artículo 33.5 de la Ley que “no será de aplicación a los intercambios de información previstos en este artículo lo dispuesto en la Ley Orgánica 15/1999 en lo referente a la exigencia de consentimiento del interesado, el deber de información al mismo y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición”, añadiendo que “serán de aplicación a los tratamientos derivados de las comunicaciones previstas en este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal”.

III

Con posterioridad a la emisión del citado informe, el marco normativo en materia de protección de datos se ha visto sensiblemente afectado por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de

2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en el seno de los recursos interpuestos por diversas asociaciones, entre ellas la propia consultante, contra el Reglamento de desarrollo de la Ley Orgánica 15/1999. A su vez, el marco se ve igualmente afectado por las Sentencias dictadas por el Tribunal Supremo en fecha 8 de febrero de 2012, por las que se resuelven los mencionados recursos.

La Sentencia del Tribunal de Justicia ha declarado expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva”. Por ello, dicho precepto deberá ser tomado directamente en cuenta en la aplicación de la normativa de protección de datos de carácter personal por los Estados Miembros, y en consecuencia por esta Agencia Española de Protección de Datos, dado que como señala el Tribunal Supremo en su sentencia de 8 de febrero de 2012 “produce efectos jurídicos inmediatos sin necesidad de normas nacionales para su aplicación, y que por ello puede hacerse valer ante las autoridades administrativas y judiciales cuando se observe su trasgresión”.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, el artículo 7 f) de la Directiva “establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado” y, en relación con la citada ponderación, el apartado 40 recuerda que la misma “dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado”.

Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán “procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión, por lo, conforme a su apartado 47 que “nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación”.

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento o por el tercero o



terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 de la Ley Orgánica 15/1999, según el cual “la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar” o si, por el contrario, dichos derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar el tratamiento de los datos de carácter personal.

En este mismo sentido, el artículo 10.2 a) del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone que será posible el tratamiento y la cesión de los datos sin contar con el consentimiento de los afectados cuando lo autorice una norma con rango de Ley o una norma de derecho comunitario y, en particular, cuando “el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre”.

En el presente caso, los criterios de ponderación impuestos por la normativa comunitaria proceden, en primer término de lo dispuesto en la propia Ley 10/2010, por cuanto su artículo 33 no sólo se refiere al posible intercambio de la información entre sujetos obligados, sino que establece una serie de límites para que dicho intercambio pueda tener lugar, así como varias condiciones adicionales exigibles a dicho tratamiento:

- Así, en primer lugar, el artículo 33.2 de la Ley limita el intercambio a la información relativa a las operaciones a las que se refieren los artículos 18 y 19, siendo además preciso que “de las características u operativa del supuesto concreto se desprenda la posibilidad de que, una vez rechazada, pueda intentarse ante otros sujetos obligados el desarrollo de una operativa total o parcialmente similar a aquella”.
- Además, el tratamiento quedará limitado expresamente a la única y exclusiva finalidad de “prevenir o impedir operaciones relacionadas con el blanqueo de capitales o la financiación del terrorismo.
- Desde el punto de vista del acceso a los datos, el mismo deberá quedar limitado, conforme al artículo 33.4 a “los órganos de control interno previstos en el artículo 26, con inclusión de las unidades técnicas que constituyan los sujetos obligados “.

- Finalmente, a fin de evitar la pérdida, alteración y acceso no autorizado a los datos objeto de intercambio, el artículo 33.5 en su párrafo segundo, establece una salvaguarda adicional, dado que “Serán de aplicación a los tratamientos derivados de las comunicaciones previstas en este artículo las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal”.

Fuera de estos supuestos, la Ley 10/2010 establece condiciones aún más severas para el intercambio de información, toda vez que el mismo únicamente podría tener lugar en los supuestos enunciados en el artículo 33.1 y previa autorización de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, cuyo acuerdo “determinará en todo caso el tipo de operación o la categoría de cliente respecto de la que se autoriza el intercambio de información, así como las categorías de sujetos obligados que podrán intercambiar la información”. Es decir, en estos supuestos, de operaciones no comunicadas al Servicio Ejecutivo y que no reúnen los requisitos del artículo 33.2, la ponderación exigirá una previa autorización específica de la Comisión de Prevención que habrá de atender específicamente a las circunstancias de cada caso concreto.

De este modo, cabría considerar que un sistema de información como el que es objeto de la presente consulta podría constituirse lícitamente, al amparo de lo dispuesto en el artículo 7 f) de la Directiva 95/46/CE, en conexión con los artículos 6.1 y 11.2 a) de la Ley Orgánica 15/1999 y 33.2 de la Ley 10/2010, siempre que el mismo cumpla los criterios de ponderación establecidos por ésta última.

IV

Pues bien, el Reglamento de funcionamiento sometido a informe específica en su articulado el cumplimiento de los criterios señalados, tanto en lo referente a los datos que se incluirán en el sistema, como a la finalidad del tratamiento y uso posterior de los datos, como a los accesos previstos, limitados a los órganos de control regulados por el artículo 26 de la Ley 10/2010, como finalmente a la necesaria implantación de las medidas de seguridad de nivel alto.

Pero además, esos criterios tendentes a garantizar adecuadamente el derecho a la protección de datos de las personas cuyos datos sean incluidos en el fichero común y, en consecuencia, objeto de consulta por los sujetos obligados, se ven además reforzados por otra serie de garantías adicionales que las normas de funcionamiento sometidas a informe vienen a establecer, y que pueden resumirse en las siguientes:

- El establecimiento de compartimentos diferenciados atendiendo a la distinta naturaleza de los sujetos obligados intervinientes, lo que supone una limitación adicional de los supuestos de acceso a los datos, limitados a los órganos de control de los sujetos



obligados de la misma naturaleza que el informante.

- El establecimiento de plazos sumamente reducidos, prácticamente de inmediatez, para la inclusión y baja de los datos en el sistema en caso de apreciarse, en cuanto a esta última acción, la existencia de un error en la información aportada o, en particular, de producirse la devolución de la operación por parte del Servicio Ejecutivo.
- La clarificación de que la información contenida en el fichero no puede determinar por sí sola la negativa a la operación solicitada, sino que deberá suponer la realización del examen especial al que se refiere el artículo 17 de la Ley 10/2010, en conexión con la prohibición de decisiones personales automatizadas establecida en el artículo 13 de la Ley Orgánica 15/1999.
- La existencia de los denominados coordinadores, cuya designación será obligatoria para los intervinientes, encargados expresamente del control de los accesos y consultas al fichero, a fin de que sólo puedan acceder a los datos las personas integrantes del órgano de control y únicamente para la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo.
- El establecimiento de un procedimiento de contestación a las solicitudes de ejercicio de los derechos previstos en la normativa de protección de datos en que se clarifique a los solicitantes la base legal que determina su denegación, al amparo del artículo 33.5 de la Ley 10/2010 y se haga constar el derecho de los afectados de solicitar la tutela de esta Agencia.
- La creación de un órgano específico encargado de velar por el efectivo cumplimiento de las normas de funcionamiento, del que formarán parte, en representación de los intervinientes, personas integradas en su órgano de control creado conforme al artículo 26 de la Ley 10/2010.
- El establecimiento de un régimen de infracciones y sanciones como consecuencia del incumplimiento de las reglas establecidas por las normas de funcionamiento que pueden implicar la exclusión e la participación en el sistema de quienes lleven a cabo incumplimientos de extrema gravedad como los descritos en el texto.

En consecuencia, el sistema introduce una serie de medidas y garantías que permiten entender minimizado el riesgo que el tratamiento pudiera

conllevar en los derechos y libertades del interesado, y en particular en su derecho fundamental a la protección de datos de carácter personal, lo que permite concluir que la creación del sistema y los tratamientos derivados del mismo se encuentran amparados por la normativa vigente en materia de protección de datos de carácter personal.

V

Deben, no obstante, efectuarse ciertas consideraciones referidas al texto de las normas de funcionamiento del fichero, que pudieran mejorar o clarificar aún en mayor medida las garantías a las que se ha venido haciendo referencia a lo largo del presente informe:

- En primer lugar, en el apartado 8.1, convendría clarificar que las cesiones de datos a autoridades judiciales, policiales y administrativas competentes se refiere a las que ostenten esta competencia “en materia de prevención del blanqueo de capitales y la financiación del terrorismo”, habida cuenta de la naturaleza del fichero y la finalidad del mismo.

- Cabría igualmente especificar en el artículo 10, aunque se derive del contexto, que serán de aplicación a los canales, soportes y formato de notificación que se especificarán en el Manual Técnico del Repositorio las medidas de seguridad de nivel alto previstas en la normativa de protección de datos de carácter personal, dado lo establecido en el artículo 33.5 de la Ley 10/2010.

- Sería conveniente que se reforzasen aún más las garantías de cumplimiento por los miembros de las Comisiones de control reguladas por el artículo 14 de los deberes de secreto impuestos por las normas de funcionamiento.

- Del mismo modo, convendría establecer un procedimiento de acceso a los datos por los miembros de las Comisiones que garantizase una minimización de la información objeto de acceso, especialmente en la tramitación del procedimiento sancionador al que se refiere el artículo 15.

- Por último, podría ser conveniente que se especificase en el régimen sancionador algún tipo de consecuencia extraordinaria en caso de comisión de dos o más infracciones graves, dado que en todos los tipos descritos la gravedad de los incumplimientos (desvío de finalidad, falsedad o acceso por terceros no autorizados) es especialmente reforzada. A nuestro juicio, la comisión de una segunda infracción de esta naturaleza debería llevar aparejada la expulsión definitiva del sistema.