La consulta plantea diversas cuestiones respecto a la aplicación de lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a la creación de un fichero con la finalidad de llevar un control sobre operaciones fallidas fraudulentas, por parte del departamento encargado de gestionar las compras a través de medios electrónicos de la entidad consultante.

I

Se consulta, en primer término, si la inclusión en un fichero de los datos personales relacionados con operaciones fallidas fraudulentas podría fundarse en lo previsto en el artículo 6.2 de la Ley Orgánica 15/1999 conforme al cual *"No será preciso el consentimiento cuando los datos de carácter personal (…) se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento"*

A este respecto, cabe señalar que dicha excepción ampararía la inclusión en un fichero de los datos de quienes efectúen compras por medios electrónicos a la entidad consultante con la finalidad en tal precepto prevista. Sin embargo, la finalidad de inclusión de los datos personales resultantes de las operaciones fallidas fraudulentas no parece ser exclusivamente la de mantenimiento o cumplimiento de la operación comercial sino la de conservar tales datos para impedir que vuelvan a producirse operaciones de tal carácter, debiendo examinarse la legitimación para dicho tratamiento de datos con fines de prevención de futuros fraudes.

Cabe así señalar que esta Agencia ha analizado la posibilidad de legitimar los ficheros de prevención de fraude en lo establecido en el artículo 7 f.) de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuyo efecto directo ha sido declarado expresamente por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, 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".

En este mismo sentido cabe señalar que el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) que resultará de aplicación a partir del 25 de mayo de 2018 señala en su considerando 45 lo siguiente "*El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. 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. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo."*

A efectos de determinar si el tratamiento de datos objeto de consulta puede venir legitimado en lo previsto en el mencionado artículo7.f) de la

Directiva 95/46 CE, debe tenerse en cuenta, tal y como señala la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, que 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 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 existe un interés legítimo perseguido por el responsable del tratamiento 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.

Así existiría un interés legítimo en tratar los datos personales resultantes de las operaciones fallidas fraudulentas que se hayan producido con la finalidad de evitar nuevos fraudes. Ahora bien, debe tenerse en cuenta que el artículo 7.f de la Directiva exige una ponderación entre el interés legítimo del responsable y los derechos fundamentales afectados, de modo que no es suficiente con apreciar la concurrencia de un interés legítimo en el responsable del tratamiento, sino que, además, la intromisión en los derechos de los afectados debe resultar proporcional, prevaleciendo, en otro caso, dichos derechos fundamentales sobre el interés legítimo que pudiera tener el responsable.

En el presente supuesto desconociéndose qué entiende el consultante por operaciones fallidas fraudulentas, en tanto que no describe qué clase de operaciones van a ser incluidas en tal concepto, ni qué datos van a ser recabados ni cómo va a llevarse a cabo el tratamiento de los mismos, no resulta posible determinar la proporcionalidad de tal tratamiento, pudiendo apuntarse únicamente que no parece que dé cumplimiento a dicho requisito la inclusión de todos los datos de los clientes del consultante en un fichero destinado al tratamiento de operaciones fallidas fraudulentas. A ello debe añadirse que cuando esta Agencia ha examinado la creación de ficheros de prevención del fraude sobre la base del interés legítimo ha tenido en cuenta para determinar que éste prevalece sobre los derechos de los afectados la existencia de garantías que atenúen los riesgos derivados de la inclusión de los afectados en tales ficheros. Cabe así mencionar entre tales garantías las relativas al refuerzo del principio de finalidad consagrado en el artículo 4.2 de la Ley Orgánica 15/1999 de modo que los datos incluidos en un fichero de prevención de fraude solamente puedan ser utilizados con tal finalidad, la especial observancia de los principios de exactitud y conservación recogidos en los números 3 y 4 del mismo artículo. Igualmente se valoraba el refuerzo del ejercicio de los derechos de acceso, rectificación, cancelación y oposición y las garantías establecidas en el artículo 13 de la Ley Orgánica 15/1999 y correlativos del Reglamento de desarrollo de la Ley Orgánica 15/1999, entre otras.

Por consiguiente, habrá que estar al cumplimiento del principio de proporcionalidad y la inclusión de garantías de los derechos de los afectados para determinar si en el presente supuesto el interés legítimo que pudiera existir en la creación del fichero prevalecería sobre los derechos de los afectados por el tratamiento.

II

Se plantea, asimismo, si el deber de información al afectado puede cumplirse incorporando la misma en la política de privacidad que se habilitará al efecto y que los usuarios debieran leer y aceptar en el marco del proceso de compra.

El artículo 5.1 de la Ley Orgánica 15/1999 dispone que *“Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante."

Respecto a la acreditación de haber dado cumplimiento al deber de información a que se refiere el artículo 5 transcrito, cabe señalar que tras la anulación de lo previsto en el artículo 18 del Reglamento de desarrollo de la Ley Orgánica 15/1999 por Sentencia de 15 de julio de 2010 del Tribunal Supremo, debe entenderse que rige la libertad de forma para acreditar el cumplimiento del deber de información, de modo que el responsable podrá demostrar por cualquier medio de prueba admisible en derecho el cumplimiento de ambos deberes.

Esta Agencia ha venido señalando que cuando se pretende dar cumplimiento a estas obligaciones en un sitio web, suelen utilizarse formularios y cláusulas a los que se accede a través de enlaces como pueden ser "aviso legal" o "política de privacidad" siendo necesario, en tal caso, que los afectados no puedan introducir dato alguno en la base de datos sin antes tener conciencia del citado aviso y "aceptarlo", haciendo "click" en el lugar correspondiente. De este modo, puede servir como acreditación del cumplimiento de dicho deber de información que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia.

III

Se consulta, por último, si, en caso de que la gestión de dicho tratamiento se llevase a cabo por una empresa externa actuando como encargado del tratamiento, sería recomendable la adopción de otras medidas distintas a las establecidas en la Ley Orgánica 15/1999 y su Reglamento de

desarrollo a fin de garantizar el cumplimiento normativo y los derechos de los usuarios.

A este respecto, cabe señalar que tanto el artículo 12 de la Ley Orgánica 15/1999 como los artículos 20 a 22 de su Reglamento de desarrollo contienen un conjunto de obligaciones en la contratación del encargado de tratamiento a las que debe en todo caso dar cumplimiento el consultante; no obstante, el responsable podrá exigir mayores garantías cuando lo tenga por conveniente, ya estén relacionadas con las medidas de seguridad a adoptar, con los mecanismos de garantía de devolución o destrucción de los datos al término del contrato, el refuerzo del deber de confidencialidad que incumbe igualmente al encargado del tratamiento y sus empleados, etc., en función de los riesgos que presenta el tratamiento.

A ello debe añadirse que el artículo 20.2 del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone que *"Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento."* Esta Agencia ha venido entendiendo que dicho precepto introduce un poder de supervisión sobre el encargado que no se limita a un especial deber de diligencia en la contratación del mismo sino que se traduce en la legitimación del responsable del fichero o tratamiento para realizar controles durante el período de vigencia del contrato para verificar el cumplimiento de las obligaciones del encargado de tratamiento y adoptar las medidas correctoras oportunas.