

La consulta plantea la conformidad con la normativa de protección de datos personales de las nuevas condiciones generales de prestación del *servicio telefónico móvil de tarjeta*, y del *servicio telefónico móvil de modalidad de contrato* de la marca YOIGO, acompañando a dichos efectos la documentación correspondiente, entre la que se incluye el documento denominado “Política de privacidad de clientes YOIGO”. A este último se accede, asimismo, a través del enlace <https://bit.ly/2JJuhDO>; <https://sobre.yoigo.com/pdf/condiciones-proteccion-datos-clientes.pdf>.

Como cuestión previa, conviene señalar que -con fecha 13 de mayo de 2020, y en el marco del Informe 0018/2020-, esta Agencia emitió su parecer en relación con otra consulta planteada por la operadora consultante, referida a la adecuación a la normativa de protección de datos personales de las *nuevas condiciones generales* de prestación del “*Servicio Telefónico y de Banda Ancha Fija*” de la marca YOIGO, que incluían la modificación de las condiciones relativas a la permanencia en el caso de contratar un paquete convergente.

En consecuencia, el presente Informe se referirá al análisis de la actual “política de privacidad” de la compañía en la versión que ahora se somete a consulta -coincidente con la accesible a través del enlace web citado más arriba-, y, en sus estrictos términos, al examen de adecuación de dicha *política* y del *resto de los documentos* que se acompañan a la normativa de protección de datos.

También como cuestión previa, debe señalarse que -según se constata-, el clausulado sobre protección de datos incorporado a los documentos sobre “condiciones generales” presentados, y referidos al *servicio telefónico móvil de tarjeta*, y al *servicio telefónico móvil de modalidad de contrato*, se incorpora, respectivamente, en las cláusulas 12 y 10 de dichos documentos.

Así, según se observa, la única diferencia existente entre dichas cláusulas, numeradas respectivamente con los números 12 y 10, se contiene en el segundo de los documentos presentados, sobre “*prestación del servicio telefónico móvil en modalidad de contrato*”, que incorpora dos subapartados -10.2-c) y 10.2-d)-, referidos respectivamente a la “*Comprobación de solvencia*” y a la “*Comunicación de los datos de impago de la deuda a ficheros comunes de solvencia*”, en aras de la mejor garantía del servicio de pospago contractual.

Finalmente, como tercera cuestión previa, debe señalarse que en los apartados **2.2 y 2.3** del documento ***“Política de privacidad de los clientes YOIGO”***, que se presenta a informe, se incorporan diversas finalidades **-que no se explicitan en los documentos sobre condiciones generales (tarjeta y contrato)** de cuyo análisis se trata-, referidas al interés legítimo de la operadora, y a otras derivadas del consentimiento de los clientes. Asimismo, en dicha política de privacidad se desarrolla con mayor amplitud la previsión relativa al ejercicio de los derechos de los afectados.

A este último documento sobre política de privacidad de los clientes de la operadora, se accede, asimismo, a través del sitio web de la consultante, mediante el enlace <https://bit.ly/2JJuhDO>; <https://sobre.yoigo.com/pdf/condiciones-proteccion-datos-clientes.pdf>, que incorpora idéntica versión que la anexada a la consulta objeto de este Informe.

I

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 -**RGPD**-), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -**LOPDGDD**- conforman el marco jurídico de referencia en España que afecta a la protección de datos de carácter personal. En estas normas se regulan los principios y fundamentos a los que deben ajustarse la recogida y tratamiento de los datos personales por cualquier persona pública o privada que lleve a cabo tratamiento de datos de carácter personal en el ejercicio de su actividad.

El citado RGPD introduce profundas modificaciones en las normas de protección de datos que afectan de forma relevante, entre otras cuestiones, al denominado principio de transparencia y derecho de información de los afectados.

Así, en primer lugar, el artículo 12.1 del RGPD establece que la información a facilitar al interesado deberá serlo “en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo”.

Por su parte, el artículo 13 en sus dos primeros apartados especifica el contenido de la citada información en los supuestos en que los datos sean recabados del afectado al que los mismos se refiere. Dicha información deberá incorporar:

- la identidad y los datos de contacto del responsable y, en su caso, de su representante;

- los datos de contacto del delegado de protección de datos, en su caso;
- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- cuando el tratamiento se base en el artículo 6, apartado 1, letra los intereses legítimos del responsable o de un tercero;
- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
- el derecho a presentar una reclamación ante una autoridad de control;
- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

En similar sentido, conforme a lo dispuesto en el artículo **11 de la LOPDGDD**:

“Artículo 11 LOPDGDD. Transparencia e información al afectado.

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el **artículo 13 del Reglamento (UE) 2016/679** facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.”

II

En la cláusula sobre *protección de datos* sometida al parecer de la Agencia -incluida como **número 12** del documento presentado sobre condiciones generales de prestación del servicio de telefonía móvil con tarjeta, y con el **número 10** del servicio de telefonía móvil en la modalidad de contrato-, se incorporan contenidos referidos a las siguientes cuestiones: ¿Quién es el responsable del tratamiento de sus datos?, ¿Con qué finalidad tratamos sus datos y bajo qué legitimación?, ¿A quién comunicamos sus datos?, Transferencias internacionales, ¿Por cuánto tiempo conservaremos sus datos? y ¿Cuáles son sus derechos?

La estructura de las citadas cláusulas -números 12 y 10, respectivamente-, se reproduce en el tercero de los documentos acompañados a la consulta, relativo a la “*política de privacidad de los clientes*” de la consultante, si bien, según se ha adelantado, este último desarrolla con mayor amplitud algunas de las previsiones contenidas en unas y otras *condiciones generales*.

En concreto, los apartados 2.2 y 2.3 de la *“política de privacidad de los clientes”*, incorporan diversas finalidades -que no se explicitan en el documento sobre condiciones generales de ninguna de las versiones sobre *“condiciones generales”* presentadas-, referidas al interés legítimo de la operadora, y a otras derivadas del consentimiento de los clientes. Asimismo, en la *“política de privacidad”* se desarrolla con mayor amplitud la previsión relativa al ejercicio de los derechos de los afectados.

A su vez, según se aprecia, tanto la versión presentada sobre *“política de privacidad de los clientes”*, como la obrante en el sitio web de la operadora, incorporan la única diferencia significativa existente entre los documentos relativos a condiciones generales de una y otra modalidad (*tarjeta y contrato*), aludiendo expresamente a la *“Comprobación de solvencia”* y a la *“Comunicación de los datos de impago de la deuda a ficheros comunes de solvencia”* en relación con la modalidad pospago (*contrato*).

En consecuencia, y habida cuenta de que en el documento sobre “política de privacidad de los clientes” de la consultante se incorporan al completo las previsiones de las cláusulas número 12 y 10 de los documentos sobre “condiciones generales” (tarjeta y contrato), añadiéndose, además, algunas otras previsiones y aclaraciones, el presente análisis se referirá al estudio de adecuación del documento “política de privacidad de los clientes” a las exigencias derivadas de la normativa de protección de datos.

La estructura de la *“política de privacidad de los clientes”* sometida a Informe, obedece al siguiente esquema: 1.) Responsable del tratamiento, 2. Finalidades del tratamiento de datos, 3. ¿A quién comunicamos sus datos?, 4. Transferencias internacionales, 5. ¿Por cuánto tiempo conservaremos sus datos? y 6. ¿Cuáles son sus derechos?

En el apartado “Responsable del Tratamiento”, se contiene una previsión de carácter general sobre dicho responsable, y se anuncia la existencia de un Delegado de Protección de Datos (DPO), con el que podrán contactar los usuarios del servicio mediante escrito dirigido al mismo por correo electrónico. Según se aprecia, idéntica previsión se contiene en la versión web incorporada al enlace <https://sobre.yoigo.com/pdf/condiciones-proteccion-datos-clientes.pdf>.

Según se observa, este apartado desarrolla con la debida amplitud y garantías los detalles relativos a la “responsabilidad de los tratamientos” realizados por la operadora consultante, adaptándose a las exigencias de concisión, transparencia e inteligibilidad, reguladas en el artículo 12.1 del RGPD, refiriendo la identidad y los datos de contacto del responsable, en los estrictos términos previstos por su artículo 13.

En lo relativo a la **finalidad de los tratamientos** de los datos de carácter personal, y a la **base legitimadora** de dichos tratamientos, en el apartado 2 de la *política de privacidad* se contienen tres subapartados, el primero de los cuales -2.1.- coincide de plano con el incluido en las condiciones generales de la modalidad “tarjeta” y “contrato”, e incorporando las menciones específicas sobre “*Comprobación de solvencia*” y la “*Comunicación de los datos de impago de la deuda a ficheros comunes de solvencia*” en relación con la modalidad pospago (contrato).

Así, según se recoge, para todos los casos (tarjeta y contrato), los datos personales podrán tratarse en el marco de la contratación y de la prestación de los servicios ofrecidos con las **finalidades** de: a) Gestión de la relación contractual, b) Prestación de servicios de telecomunicaciones (...), e) Verificación de información, f) Prevención del fraude, g) Información comercial propia, h) Fines estadísticos, y g) Libro Registro y cooperación con los agentes facultados. A su vez, y exclusivamente en lo relativo a la modalidad pospago (contrato), se recogen también las relativas a: c) Comprobación de solvencia, y d) Comunicación de los datos de impago de la deuda a ficheros comunes de solvencia.

A dichas finalidades, se añaden las enunciadas en el apartado 2.2 -derivadas del *interés legítimo* invocado por la operadora consultante-, y en el apartado 2.3, vinculadas a la prestación del *consentimiento* de los clientes afectados por los tratamientos.

De tal modo, se procede a la estructuración de *catorce (14) tipos* de finalidades, de acuerdo con una sistemática cuyo epicentro se sitúa en la base jurídica que legitima cada una de ellas, con expresa mención, en cada caso, de la concurrencia de una u otra causa de legitimación.

En concreto, las finalidades relativas a la “a) *Gestión de la relación contractual*”, y a la “b) *Prestación de servicios de telecomunicaciones*”, se vinculan a diferentes actividades que se *presumen* necesarias e inherentes a la prestación del servicio de telecomunicaciones, derivadas del propio contrato.

Así, de una parte, se vinculan a la relación contractual los tratamientos de datos necesarios para la gestión del servicio de atención al cliente, del servicio técnico y de la atención de reclamaciones; los tratamientos inherentes a los cambios en la contratación o incidencias, y los derivados de la habilitación de acceso del cliente a su área privada, de la autogestión de tarifas, y del acceso a facturas y consulta de consumos.

Y, de otra parte, se relacionan también con la prestación contractual, la conducción de la comunicación a través de una red de comunicaciones electrónicas, el establecimiento y enrutamiento de la llamada, la provisión del servicio de acceso a Internet, *el registro de*

los datos de tráfico e interconexión y su uso con el objetivo de poder proceder a su facturación o al descuento dentro del saldo disponible para las tarjetas prepago, la reclamación extrajudicial y judicial en caso de impago, la detección, gestión y resolución de incidencias y reclamaciones, y la portabilidad.

En unos y otros supuestos, se señala expresamente que la base jurídica legitimadora de estos tipos de tratamiento se fundamenta en la relación contractual, y en el caso de la portabilidad en la adopción de medidas precontractuales, lo que resulta conforme con lo dispuesto en el artículo 6.1 b) del RGPD, al devenir dichos tratamientos necesarios para la ejecución del contrato en el que el interesado es parte.

De acuerdo con el documento objeto de análisis, los datos personales de cuyo tratamiento se trata, relacionados con la *“Gestión de la relación contractual”*, son los datos identificativos, los de contacto, los datos referidos a tarifas, a servicios contratados, a consumos y uso de los servicios, a calidad del servicio, y a recargas, medios de pago y facturas emitidas.

Asimismo, para la *“Prestación de servicios de telecomunicaciones”*, además de los datos de contacto, se tratarán los datos de identificación de los dispositivos y la dirección IP, *así como los datos de localización, de tráfico y de navegación.*

Pues bien, **a los efectos de la gestión contractual** que posibilite la prestación del servicio de telecomunicaciones, el tratamiento de los *datos de navegación, tráfico y localización* por parte de la consultante deberá limitarse a lo estrictamente necesario en orden a la referida facturación o al descuento en las tarifas, sin que, en ningún caso, la base legitimadora del artículo 6.1 b) RGPD ampare otro tipo de tratamientos que, en su caso, deberán fundamentarse en alguna otra de las causas de legitimación reguladas en el artículo 6.1.

Así, con carácter general, en lo que respecta a la finalidad consistente en tratar **datos de localización** que se generen a través del uso del terminal móvil de los afectados, debe recordarse que el artículo 48.2.c) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, norma especial cuya aplicación prevalece sobre el Reglamento, dispone que:

“Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de tráfico, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos: c) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento,

la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado. Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico.”

Por consiguiente, de acuerdo con lo dispuesto en el artículo 6.1 a) del RGPD, con independencia del supuesto referido a la facturación o al descuento tarifario -que podrá basarse en las previsiones del artículo 6.1 b) del RGPD-, la base legal que permite el resto de los tratamientos de dichos datos es el consentimiento de los usuarios afectados manifestado de manera específica.

Todo ello, sin perjuicio de que -adicionalmente- la operadora consultante dé el debido cumplimiento a las obligaciones relativas a la retención de los *“datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado”*, regulado en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

En este sentido, la operadora consultante, como parte del apartado que ahora se analiza, referido a la prestación del servicio de telecomunicaciones, ha introducido la siguiente previsión:

“Adicionalmente te informamos de que, como operador de telecomunicaciones, estamos obligados a comunicar tus datos identificativos, de contacto y, en ciertas ocasiones, de localización, al Sistema de Gestión de Datos de Abonado de la CNMC por obligación legal y son proporcionados, por ejemplo, a los servicios de emergencia. También, en aquellos casos en los que lo consientas, tus datos serán introducidos en las guías de abonado y, si lo consientes, los datos de las guías podrán ser tratados con fines comerciales.”

De todo lo anterior, se extrae que la cláusula objeto de estudio *no resulta clara ni concisa, no atendiendo de manera inteligible y fácilmente accesible a las exigencias* derivadas de la aplicación de los artículos 12 y 13 del RGPD. Esto es, de la lectura del apartado *“Prestación de servicios de telecomunicaciones”*, se desprende que *se mezclan distintas bases jurídicas* que legitiman el tratamiento. Así, de una parte, la prevista en el artículo 6.1 b) RGPD referida a la ejecución de un contrato, sin que, sin embargo, se reflejen con la exactitud necesaria, los límites a los que se ha hecho anterior mención. Y, de otra parte, la prevista en el artículo 6.1. c) RGPD, relativa al supuesto en que el tratamiento resulte necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, que justifica la conservación de los datos de tráfico y localización por parte de las operadoras -durante el plazo

de doce meses- en virtud de lo dispuesto en los artículos 3, 4 y 5 de la Ley 25/2007, de 18 de octubre.

Todo ello puede provocar que el destinatario de la información no sepa con claridad si el tratamiento de los datos es necesario para la ejecución del contrato/servicio, o si, por el contrario, deberá otorgar su consentimiento, además de arrojar dudas acerca de la base jurídica aplicable -*ex artículo 6.1.c)*- en relación con la retención de los datos de tráfico y localización.

En consecuencia, para que se cumpla con el principio de transparencia, que implica el uso de información concisa, transparente, inteligible, y con un lenguaje, claro y sencillo, debe modificarse el texto del apartado presentado a informe, de modo que (i) se especifiquen claramente los límites del tratamiento de datos de tráfico y localización específicamente vinculados a la facturación, (ii) se atribuya con claridad al consentimiento la posibilidad de utilización de dichos datos para otras finalidades distintas, y (iii) se especifique claramente que, fuera de los anteriores supuestos, la conservación de datos de tráfico y localización se circunscribe a lo dispuesto en la normativa que resulta aplicable.

A su vez, la consultante deberá estar a los principios relativos al tratamiento de datos recogidos en el artículo 5 del RGPD, y, muy especialmente, a lo dispuesto en relación con el denominado “principio de minimización de datos”, de acuerdo con el cual “Los datos personales serán: (...) c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”, de modo que cualquier tratamiento de dichos datos que no resulte imprescindible en relación con la *prestación del servicio de telecomunicaciones*, deberá quedar amparado, en su caso, por alguna otra de las bases legitimadoras de los tratamientos previstas en el artículo 6 del RGPD.

Asimismo, la “Política de privacidad de clientes” de la operadora, se refiere a las finalidades relativas a: e) Verificación de información, f) Prevención del fraude, g) Información comercial propia, h) Fines estadísticos, informando de que en todos estos casos la base legitimadora del tratamiento entronca con el “interés legítimo” de la operadora.

Pues bien, en cuanto a la “verificación de información” y la “prevención del fraude”, la concurrencia del dicho interés legítimo -ostentado por la consultante- resulta claro e incontrovertido, articulándose en aras de la prevención del fraude en la contratación, y refiriéndose únicamente al tratamiento de los datos estrictamente necesarios para dicho fin.

Así, la verificación de la exactitud de los datos aportados por los clientes y la adhesión al “Sistema Hunter” de lucha contra el fraude, constituyen herramientas lícitas, proporcionadas y adecuadas en orden a la mejor garantía de los derechos de los afectados y a la salvaguarda de los intereses de la

propia consultante, al objeto de detectar la existencia de información potencialmente fraudulenta en el proceso de aprobación del servicio.

El conjunto de estas medidas -adoptadas *ad cautelam* y concretadas en determinadas formas de tratamiento de datos de carácter personal- encaja en las previsiones del artículo 6.1 f) del RGPD, cuando dispone que el tratamiento será lícito cuando sea *“necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño”*.

En conclusión, tanto la referencia al “interés legítimo”, como los medios implementados en orden a la verificación de la exactitud de los datos facilitados por el cliente -a los que se refiere la cláusula incorporada al documento objeto de informe-, resultan conformes con los requisitos inherentes a la base jurídica del tratamiento del citado artículo 6.1 f) del RGPD.

A su vez, la consultante justifica la concurrencia de su interés legítimo en relación con finalidad relativa al envío de “Información comercial propia”, procediendo a la personalización de ofertas y, en último término, al ofrecimiento de productos y servicios propios para subvenir a las necesidades y deseos de sus clientes.

A este respecto, conviene recordar que, en el envío de comunicaciones comerciales personalizadas -siempre que dichas comunicaciones sean relativas a servicios o productos de la marca del consultante sobre los cuales el cliente tenga una expectativa razonable de recibirlos como cliente-, y tratándose de comunicaciones electrónicas, el artículo 21 de la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico -norma especial cuya aplicación prevalece sobre el Reglamento-, exige el consentimiento expreso del interesado, *salvo que se trate de productos y servicios similares* a los ya contratados por el usuario.

De este modo, cuando se utilicen *otros canales de comunicación* esta Agencia ha venido entendiendo que, por analogía, resulta posible efectuar publicidad sobre productos o servicios similares a los contratados, pudiendo existir un “interés legítimo” siempre y cuando se haga una interpretación razonable de lo que debe ser un *producto o servicio similar* al previamente contratado, ***no extendiéndose a aquéllos respecto de los que no pueda aplicarse una identificación lógica*** basada en la expectativa razonable del cliente. En consecuencia -dentro de los límites expuestos-, estos tratamientos se fundamentarían en lo dispuesto en el artículo 6.1 f) del Reglamento General de Protección de Datos.

A su vez, en lo que respecta al envío de comunicaciones comerciales, la cláusula sometida a informe especifica claramente el posible ejercicio del derecho de oposición, lo cual resulta conforme con la normativa aplicable.

En cuanto a los “Fines estadísticos”, en el documento sometido a informe se prevé que determinados datos **previamente anonimizados** puedan ser utilizados con fines estadísticos o de investigación sobre la base del interés legítimo de la consultante.

A este respecto, se ha de señalar que, sobre los datos previamente anonimizados, no existirán tratamientos de datos de carácter personal en el sentido recogido por la normativa de protección de datos.

Así, de acuerdo con el contenido de las “Definiciones” del artículo 4 del RGPD, para que exista tratamiento de datos de carácter personal -según se prevé en su punto 2-, se requiere la realización de *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”*.

En consecuencia, cuando dicha información de carácter personal se encuentre sometida previamente a un procedimiento de disociación, no resultará aplicable lo dispuesto en dicho Reglamento -RGPD-, decayendo sus previsiones en relación con la información “anonimizada” objeto de tratamiento. En resumen, la normativa de protección de datos no resulta aplicable a los tratamientos sometidos a un previo procedimiento de disociación.

En este sentido, en el Considerando (26) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se contiene la interpretación de lo que ha de entenderse por información anonimizada, delimitando claramente dicho concepto del relativo a la “seudonimización” de datos, a saber:

“(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios

para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.”

Contrario sensu, el Considerando (28) del RGPD, interpreta la aplicación efectiva de la normativa de protección de datos a los tratamientos de datos seudonomizados, al disponer que *“La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.”*

Atendiendo a lo que acabamos de indicar, para que un procedimiento de anonimización pueda ser considerado suficiente a los efectos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, será necesario que de la aplicación de dicho procedimiento resulte imposible identificar un determinado dato con su sujeto determinado. En este sentido, las disposiciones internacionales reguladoras de la protección de datos de carácter personal vienen a considerar que el afectado no será determinable cuando su identificación exija un esfuerzo desproporcionado que haga imposible, en la práctica, identificar a la persona física titular de los datos personales previamente tratados por el responsable.

No obstante lo anterior, conviene insistir en la clara distinción existente de ambas figuras. Así, mientras a través de la disociación se impide la identificación del sujeto afectado, y se sitúa la información objeto de tratamiento fuera del ámbito de aplicación de la normativa de protección de datos, la seudonimización requiere la adopción de medidas técnicas y organizativas necesarias para garantizar que se aplique el RGPD al tratamiento correspondiente, pero mantiene por separado la información adicional para la atribución de los datos personales a una persona concreta (*ex Considerando 29 RGPD*), quedando los tratamientos de datos sometidos al régimen del RGPD.

En consecuencia, por parte de la consultante deberá examinarse si el tratamiento de la información **estadística** generada se encuentra sometido o no a la normativa de protección de datos, determinándose si los datos tratados van a vincularse o no a datos personales que identifiquen de algún modo a los afectados.

A su vez, deberá realizarse una mención específica a los plazos previstos en relación con la finalidad estadística, y, en su caso, a la posibilidad

de que el tratamiento derivado de la pretendida finalidad considere la existencia de diversos plazos en función de la eventual concurrencia de distintas bases jurídicas que amparen el tratamiento estadístico.

El apartado 2.1. del documento que se analiza, se refiere también a los tratamientos de datos necesarios para la llevanza del *“Libro Registro y cooperación con los agentes facultados”, en su doble vertiente* de clientes prepago -tarjeta- y pospago -contrato-, con expresa mención de la normativa aplicable que exige la recogida y tratamiento de determinados datos de carácter personal.

En concreto, se alude a lo dispuesto por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, informándose a los clientes sobre la tipología de dichos datos, sobre la finalidad de los tratamientos, y sobre los destinatarios de las cesiones de datos legalmente establecidas.

Tal y como se refleja en el documento presentado, la base jurídica que legitima el tratamiento de estos datos es la recogida en la letra c) del artículo 6.1 del RGPD, que dispone que el tratamiento será lícito cuando resulte *“necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”*.

A su vez, y ***exclusivamente en lo relativo a la modalidad pospago*** (contrato), el documento sobre “política de privacidad” presentado a informe, se refiere a las finalidades relativas a la *“c) Comprobación de solvencia”, y a la “d) Comunicación de los datos de impago de la deuda a ficheros comunes de solvencia”,* que vincula a la satisfacción de sus intereses legítimos.

A este respecto, debe reiterarse que, según dispone el apartado f) del artículo 6.1, del RGPD, referido a la *“Licitud del tratamiento”*:

“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: (...) f) el tratamiento es necesario para la satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.”

Así, en relación con el tratamiento de datos referidos a ambas finalidades, la entidad consultante alude a su interés legítimo, que justificaría tanto (i) *-de manera previa* a la contratación- la comprobación de determinados

datos de carácter personal necesarios para la garantía de sus intereses, como (ii) -posteriormente, en caso de impago- la comunicación de los datos de sus clientes a los ficheros de solvencia patrimonial y crédito.

A nuestro juicio, tanto la referencia al “interés legítimo”, como los medios implementados en orden a la comprobación de solvencia de los clientes, y a la eventual incorporación de sus datos a ficheros de solvencia patrimonial y crédito en los supuestos establecidos legalmente-, resultan conformes con los requisitos inherentes a la base jurídica del tratamiento incardinada en el citado artículo 6.1 f) del RGPD.

Específicamente, en relación tanto (i) con la “consulta previa”, como (ii) con la “comunicación posterior” a los sistemas de información crediticia, la operadora consultante hace especial mención a lo establecido en la LOPDGGD.

A este respecto, debe señalarse que, según disponen el artículo 20 de la Ley Orgánica 3/2018, de 5 de diciembre:

“Artículo 20. Sistemas de información crediticia

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.”

III

En el apartado 2.2. de la política de privacidad de la compañía consultante, se refiere la posibilidad del análisis del *“uso que el cliente hace de los servicios contratados”* a fin de mejorarlos, ampliarlos y desarrollar nuevos servicios, tarifas y/o promociones, adoptando las medidas oportunas para garantizar *el menor impacto* en el derecho a la protección de datos del cliente. Este tipo de acciones pretenden fundamentarse en el “interés legítimo” de la operadora, quien, en el documento presentado a informe, señala que, a los pretendidos efectos, se tratarán los datos estrictamente necesarios a dicho fin, procediendo a la pseudonimización

de la información con datos de carácter personal, y garantizando, en todo caso, el derecho de oposición del cliente.

Pues bien, a nuestro juicio, la citada cláusula (2.2.) resulta **vaga y confusa**, por cuanto, sin perjuicio de que se refiera algún supuesto concreto en aras de su concreción, no se infiere con la claridad exigible qué debe entenderse por el *“uso que el cliente hace de los servicios contratados”*.

Al tiempo, si como señala la consultante, este tipo de tratamientos requieren de un previo análisis y evaluación de impacto, se extrae que estos deberían precisarse con el oportuno detalle, sin que el invocado “interés legítimo” pueda servir para fundamentar el tratamiento de datos más allá de las previsiones establecidas legalmente, y, muy especialmente, en lo relativo a evaluaciones de impacto, de lo dispuesto por el artículo 35 del RGPD:

Artículo 35. Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
(...)

7. La evaluación deberá incluir como mínimo: a) **una descripción sistemática de las operaciones de tratamiento previstas** y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.” (la negrita es nuestra)

En consecuencia, por parte de la operadora consultante deberá precederse a la concreción singularizada y sistemática de las acciones que pretenda emprender sobre la base de su “interés legítimo” y que tenga por objeto el análisis del *“uso que el cliente hace de los servicios contratados”*, detallando, al menos, las operaciones de tratamiento previstas, los fines que persiga con su desarrollo, e, incluso, la naturaleza y características del interés legítimo que persiga con este tipo de tratamientos.

Únicamente, de este modo, se dará el debido cumplimiento a las previsiones del apartado f) del artículo 6.1, del RGPD, referido a la “*Licitud del tratamiento*”, anteriormente transcrito.

En el apartado 2.3 del documento sobre “política de privacidad de clientes” se describen los tipos de tratamiento de datos cuya base de legitimación se obtiene a través del *consentimiento* otorgado por el cliente. Así, a) El envío de información comercial de otros servicios de (...) o de otras empresas del Grupo, b) El envío de información comercial de terceros, c) El perfilado y enriquecimiento de bases de datos con fines comerciales, d) El tratamiento de los datos de tráfico y navegación, y e) El tratamiento de los datos de localización.

Según se expuso en el **punto II** de este Informe, en relación con las empresas del grupo y dentro de los límites de la interpretación razonable a la que se hace mención en los párrafos precedentes, tendrá cabida la comunicación de los datos de carácter personal basada en el “interés legítimo”. Para el resto de los supuestos, tal y como prevé la consultante en su “política de privacidad”, resultará necesario que los clientes afectados *otorguen previamente su consentimiento* expreso para el tratamiento, siendo también necesario dicho consentimiento para la elaboración de perfilados y de caracterizaciones.

Asimismo, tal y como prevé la operadora consultante, en lo que respecta a la elaboración de perfiles y enriquecimiento de las bases de datos propias, así como en relación con el tratamiento de los datos de *tráfico, navegación y localización*, debe informarse a los interesados específicamente sobre la necesidad de consentir expresamente dichos tratamientos de sus datos de carácter personal, *dejando siempre a salvo la posibilidad de revocar posteriormente dicho consentimiento*.

En concreto, en relación con el perfilado y enriquecimiento de bases de datos, la operadora consultante prevé que el cliente **pueda graduar** su consentimiento sobre el tipo de datos en consideración a su origen. Así, según se señala en la “política de privacidad”, dichos datos podrían provenir de (i) bases de datos de fuentes de acceso público, (ii) de criterios geográficos (provincia, localidad, código postal, área censal), (iii) de información catastral, (iv) de datos sociodemográficos (renta media o tasa de paro por distrito o población en la que reside), (v) de datos recibidos de las interacciones digitales realizadas por los clientes, por ejemplo, por medio del uso de cookies, píxeles o cualquier tecnología de seguimiento, y (vi) de datos de interacciones con otros productos y servicios digitales como son la APP de la consultante, cookies y píxeles de sus páginas webs, actuaciones que realiza en sus redes sociales, etc.

En consecuencia, para todos estos supuestos, *debe informarse* que el tratamiento de los datos requerirá del consentimiento de las personas afectadas, orientando específicamente a los interesados sobre la *posibilidad de revocar posteriormente dicho consentimiento*.

En conclusión, en relación con dicha exigencia -derivada de lo dispuesto en el artículo 6.1 a) del RGPD-, deberá incorporarse la correspondiente previsión en el clausulado sometido a informe, garantizando que el tratamiento de los datos de carácter personal de los afectados para dichos fines resulta consentido, en los términos de los artículos 4.1-11 y 7 del RGPD. De acuerdo con dichos preceptos, dicho consentimiento debe ser informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

En este sentido, en cuanto a la posibilidad de que el consentimiento se otorgue únicamente en relación con alguno o algunos de los tipos de datos a los que se refiere la “política de privacidad”, *deberá establecerse claramente dicha opción*, por medio de un sistema claro, sencillo e inteligible, que responda a las exigencias del artículo 7.2 del RGPD, cuando dispone que:

“2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma **que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo**. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.” (la negrita es nuestra)

Así, por ejemplo, sólo a través del “marcado” expreso e independiente de todas o alguna de las opciones anunciadas, quedarán legitimadas las diferentes actuaciones de la operadora basadas en el consentimiento de sus clientes.

IV

Bajo el título ¿A quién comunicamos sus datos? (apartado 3), la cláusula que se informa refiere la existencia de una pluralidad de destinatarios -cesionarios de la información con datos de carácter personal-, y acompaña un cuadro estructurado de acuerdo con el tipo de datos comunicados y la habilitación legal que, en cada caso, ampara la cesión de dicha información. Del análisis de las cesiones previstas, se infiere su conformidad con la normativa de protección de datos.

El documento objeto de informe se refiere también de manera expresa a las transferencias internacionales de datos (apartado 4). Así, según se prevé en dicha “política de privacidad”, en el epígrafe “Transferencias internacionales”, la operadora consultante no tiene previsto llevar a cabo transferencias

internacionales de datos personales de clientes con carácter general, si bien, “puede contar con algún proveedor que requiera tratar datos de clientes desde fuera del Espacio Económico Europeo, tales como algún servicio de atención al cliente o soporte, en base a la ejecución del contrato”. Para estos casos asegura que cuenta con garantías adecuadas, ***pero no se refiere específicamente al tipo de estas.***

De tal modo, no se señalan con la debida claridad las garantías de cuya adopción se trata, por lo cual para dar el debido cumplimiento de las obligaciones establecidas en el referido artículo 13.1 f) RGPD, dirigidas a la adopción de las garantías adecuadas y apropiadas en orden a la realización de dichas transferencias y a los medios para obtener una copia de estas o al hecho de que se hayan prestado las citadas garantías, deberá adaptarse la cláusula objeto de este análisis a las previsiones de dicho precepto.

El apartado 5 del documento objeto de este Informe, se refiere a la “conservación de los datos” personales de los afectados. Con carácter general, se dispone la conservación de los datos por la operadora mientras se mantenga la relación contractual, procediéndose posteriormente al bloqueo de los datos.

Pues bien, a este respecto, la consultante deberá estar a lo que resulte de la aplicación del artículo 32 de la **LOPDGDD**, cuando dispone que:

“Artículo 32. *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.
2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.
(...)”

Finalmente, en el documento (apartado 6) se hace referencia a la posibilidad de ejercicio de los derechos en materia de protección de datos, con indicación concreta de la fórmula y de los medios puestos al servicio de su efectividad.

La cláusula sometida al parecer de la Agencia hace concreta referencia a los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad establecidos en el Reglamento General de Protección de Datos -artículos 12 a 23 RGPD-, que podrán ejercitarse conforme a lo dispuesto por dicha normativa reguladora. A su vez, en este mismo apartado se reconocen de manera expresa el derecho a “revocar” el consentimiento prestado, y el derecho a interponer una “reclamación ante la Agencia Española de Protección de Datos.

El análisis de idoneidad de dicha cláusula resulta afirmativo, habida cuenta su conformidad con las exigencias derivadas de la normativa aplicable, y refiriéndose con la suficiente claridad y detalle a dichos derechos y a la forma de su ejercicio.

V

En conclusión, es preciso que se modifique el documento objeto del presente informe en los términos que se han venido señalando, a fin de garantizar el adecuado cumplimiento de lo dispuesto en el artículo 13 del Reglamento General de Protección de Datos.

Asimismo, dichas modificaciones deberán surtir efecto en la versión web de la “política de privacidad de clientes” de la consultante, que se ofrece en el sitio web <https://sobre.yoigo.com/pdf/condiciones-proteccion-datos-clientes.pdf>, a cuyo contenido -si bien no se ha sometido formalmente al presente Informe-, se ha accedido a efectos de establecer las oportunas concordancias, debiendo adaptarse dicho contenido a lo expuesto en el cuerpo de este Informe.

En todo caso, estas consideraciones sobre la política de privacidad lo son a los exclusivos efectos del presente informe, cuyo objeto esencial es la valoración de las cláusulas aportadas en los contratos, de forma que no excluye cualquier actuación posterior que haya de llevar a cabo esta Agencia en relación con la citada política y con los tratamientos llevados a cabo por la consultante dentro de su ámbito.