

INFORME SOBRE POLÍTICAS DE PRIVACIDAD EN INTERNET

ADAPTACIÓN AL RGPD

SEPTIEMBRE 2018



ÍNDICE

1	RESUMEN EJECUTIVO	3
2	INTRODUCCIÓN.....	5
3	OBJETIVOS	6
4	ALCANCE Y METODOLOGÍA	7
5	ESTADO DE SITUACIÓN	8
5.1	INFORMACIÓN PROPORCIONADA AL INTERESADO	8
5.2	TRATAMIENTO BASADO EN EL CONSENTIMIENTO DEL INTERESADO	15
5.2.1	CONSENTIMIENTO INFORMADO	15
5.2.2	SOLICITUD DEL CONSENTIMIENTO	17
5.3	PRESENTACIÓN DE LA INFORMACIÓN AL INTERESADO	19
5.4	DELEGADO DE PROTECCIÓN DE DATOS.....	20
5.5	OBSERVACIONES GENERALES.....	21
6	RECOMENDACIONES.....	23
6.1	INFORMACIÓN PROPORCIONADA AL INTERESADO	23
6.2	TRATAMIENTO BASADO EN EL CONSENTIMIENTO DEL INTERESADO	28
6.2.1	CONSENTIMIENTO INFORMADO	28
6.2.2	SOLICITUD DEL CONSENTIMIENTO	30
6.3	PRESENTACIÓN DE LA INFORMACIÓN AL INTERESADO	31
6.4	DELEGADO DE PROTECCIÓN DE DATOS.....	33

1 RESUMEN EJECUTIVO

El presente informe tiene como objeto verificar, en el entorno *online*, la adaptación de las empresas a la nueva normativa aplicable desde el pasado 25 de mayo en materia de protección de datos personales y dictar recomendaciones para su aplicación a los distintos sectores.

Debido a la magnitud de la materia analizada, se ha seleccionado como muestra y se ha centrado el análisis en entidades de cuatro sectores: hoteles, transporte, comercio electrónico y seguros. Asimismo, también se han revisado empresas dedicadas a la venta de entradas *online* y a los servicios de música y contenidos de transmisión en tiempo real.

Para este informe, se ha analizado el cumplimiento del deber de informar al interesado cuando se obtienen sus datos personales y, para aquellos casos en que el tratamiento de datos personales esté basado en el consentimiento del interesado, la información ofrecida para que ese consentimiento sea informado, así como el modo de obtener ese consentimiento. También se ha efectuado un análisis sobre la figura del Delegado de Protección de Datos, en aquellos casos en que se contara con uno.

A tal fin, se han revisado las políticas de privacidad y formularios de recogida de datos personales de diversas entidades, utilizando para ello un cuadro que ha permitido analizar y comparar los análisis efectuados para cada entidad.

Como resumen, cabe destacar que en general se ha detectado que los documentos que detallan las políticas de privacidad son demasiado extensos y no facilitan que un usuario medio finalice su lectura ni que la comprenda. Esto resulta principalmente notorio cuando se enumeran las finalidades para las que se recogen los datos personales, que suelen explicarse detalladamente, lo cual en ocasiones puede resultar confuso para el interesado.

También se ha detectado que no se mencionan o no se explican correctamente las bases que legitiman el tratamiento de datos personales en cuestión, dado que a veces se incluye como interés legítimo lo que en realidad es tratamiento necesario para la ejecución del contrato, o bien, se encuadra dentro de interés legítimo lo que en realidad no lo es.

En cuanto al lenguaje utilizado en las políticas de privacidad, se han encontrado expresiones ambiguas o demasiado genéricas, que no aportan información en sí al interesado y que pareciera que solo se utilizan para dar una apariencia de cumplimiento de la normativa aplicable.

Respecto a la solicitud del consentimiento, en su caso, se ha observado que se utiliza mucho la recogida “en bloque”, es decir, que no se recoge el consentimiento para cada una de las finalidades de tratamiento de datos personales, sino que se acude a la fórmula *“He leído y acepto la política de privacidad”*.

Como recomendaciones generales para cumplir con la normativa vigente, se aconseja a las empresas revisar la extensión de sus documentos sobre privacidad, a fin de que cumplan con el deber de informar al interesado sin que sean tan extensos que produzcan el efecto contrario. Se sugiere la utilización de una primera capa en la que proporcione información resumida y una segunda capa con información más detallada.

También se recomienda, entre otras medidas, que se agrupen las finalidades para las que se solicita el consentimiento del interesado, de modo que no se trate de una recogida de consentimiento “en bloque” pero que tampoco resulte demasiado engorroso controlar la utilización de sus datos.

Además, se hacen recomendaciones en cuanto al lenguaje utilizado y a la importancia de sintetizar y exponer la información de forma correcta.

Por último, cabe destacar que, si bien se nota un esfuerzo por parte de las entidades por actualizar sus apartados sobre Privacidad y sus formularios de recogida de datos, no es menos cierto que todavía se aprecia cierta resistencia a pasar de un modelo anteriormente basado en el consentimiento, en el que bastaba con un consentimiento tácito, a un nuevo modelo en que se amplía la información que debe proporcionarse al interesado y que exige una clara acción positiva para consentir el tratamiento de sus datos personales. Un nuevo modelo que otorga más garantías al interesado para controlar la utilización de sus datos por parte de las distintas entidades y que contempla (y prima) otras bases distintas para legitimar este tratamiento, tales como el interés legítimo y el desarrollo de la relación contractual.

2 INTRODUCCIÓN

El Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (en lo sucesivo, RGPD), publicado en mayo de 2016 y aplicable desde el 25 de mayo de 2018, es una norma de aplicación directa en la Unión Europea, 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.

El RGPD desplaza, en todo lo que a él se oponga, a la Ley Orgánica de Protección de Datos (en adelante, LOPD) y a su reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, e introduce una serie de cambios y novedades a los cuales es necesario adaptar los actuales tratamientos.

Entre las novedades, se generaliza el concepto de “tratamiento” (artículo 4.2 del RGPD) y se incorporan requisitos adicionales en cuanto a la necesidad de informar a las personas interesadas.

Al respecto, los artículos 13 y 14 del RGPD detallan la información que debe facilitarse al interesado cuando los datos sean recogidos directamente de éste o no, respectivamente.

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el responsable del tratamiento. Si los datos se obtienen directamente del interesado, debe ponerse a su disposición la información en el momento en que se soliciten los datos, previamente a la recogida o registro. Si no se obtienen del propio interesado, se le debe informar antes de un mes desde que se obtuvieron los datos personales, o antes o en la primera comunicación con el interesado, o antes de que los datos (en su caso) se hayan comunicado a otros destinatarios.

Otra novedad es la que recoge el artículo 12.1 del RGPD, que establece que la información facilitada al interesado debe proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

En cuanto al tratamiento de datos basado en el consentimiento del interesado, el artículo 7 del RGPD indica que el responsable del tratamiento deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales. Si el consentimiento se otorgara en el contexto de una declaración escrita que refiera también a otros temas, se obliga a que la solicitud de consentimiento se distinga claramente de los demás asuntos y se presente de forma inteligible, de fácil acceso y utilizando un lenguaje claro y sencillo.

Se exige, además, que se le proporcione información adicional al interesado, entre otros, cuáles serán las categorías de datos a tratar, las finalidades para las que se

solicita el consentimiento y el derecho a retirar el consentimiento en cualquier momento¹.

En cuanto al modo de obtener el consentimiento del interesado para el tratamiento en cuestión, el considerando 32 del RGPD dispone que este *“debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen”* y que *“el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento”*. Asimismo, se exige que el consentimiento se otorgue *“para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos”*. Por último, establece que *“si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta”*.

3 OBJETIVOS

Ante la reciente aplicación del RGPD, con el objeto de verificar la adaptación de las empresas en el entorno *online* a la nueva normativa aplicable y para dictar recomendaciones para su aplicación a los distintos sectores, la Agencia Española de Protección de Datos (AEPD) ha realizado una evaluación de distintas políticas de privacidad, a fin de comprobar que se cumple con el deber de información al interesado. Asimismo, para aquellos casos en que el tratamiento de datos personales estuviera basado en el consentimiento del interesado, además de comprobar que ese consentimiento sea informado, se ha analizado el modo de obtener ese consentimiento del interesado para el tratamiento de sus datos personales. Por último, se ha efectuado un análisis en relación con la información facilitada sobre la figura del Delegado de Protección de Datos, en aquellas entidades en que se cuenta con uno.

Ante la magnitud de la materia objeto del presente informe, y como muestra, se han analizado entidades pertenecientes a cuatro sectores: hoteles, transporte, comercio electrónico y seguros. También se han revisado empresas dedicadas a la venta de entradas *online* y a los servicios de música y contenidos de transmisión en tiempo real.

¹ Grupo de Trabajo del Artículo 29 sobre Protección De Datos, “Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679” (wp259rev.01): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

La actuación de la AEPD para la realización del presente análisis está basada en las funciones que le confiere el artículo 57.1.a) del RGPD (*“controlar la aplicación del presente Reglamento y hacerlo aplicar”*) y 57.1.d) (*“promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento”*).

4 ALCANCE Y METODOLOGÍA

La evaluación sobre la adaptación al RGPD de las políticas de privacidad en Internet se estructura en torno a los cuatro sectores analizados (hoteles, transporte, comercio electrónico y seguros) y se articula analizando los mismos asuntos en cada uno de ellos.

Asimismo, el presente informe incluye un apartado de estado de situación, en el que se reflejan los resultados del análisis de las políticas de privacidad en cuanto a la adecuación a la normativa de protección de datos, y un apartado de recomendaciones a la vista de los hallazgos encontrados.

Desde el punto de vista metodológico, la evaluación se ha realizado mediante la comparación, en el entorno *online*, de la información proporcionada en las políticas de privacidad de las empresas objeto de la presente muestra y de los formularios utilizados para obtener el consentimiento del interesado cuando fuera necesario.

Se han revisado las páginas web de varias entidades pertenecientes a distintos sectores: hoteles (algunas pequeñas y medianas empresas), transporte de pasajeros (en general, grandes empresas), comercio electrónico (grandes y medianas empresas), seguros (en su mayoría, grandes empresas) y se efectuó el análisis también de empresas dedicadas a la venta de entradas *online* y a los servicios de música y contenidos de transmisión en tiempo real (en general, empresas de mediano tamaño). Asimismo, algunas de las empresas analizadas pertenecen al sector público.

A fin de homogeneizar el análisis de entidades de tan distintos sectores, se ha elaborado un cuadro para la recogida de información de las entidades, que permite comparar la información que debe facilitarse al interesado al momento de la recogida, así como la información adicional que debe proporcionarse en caso de solicitar el consentimiento. Además, se ha recogido el modo de obtención de este consentimiento y cómo se cumple con la obligación de informar. Por último, se ha analizado también la figura del Delegado de Protección de Datos, en aquellas entidades en las que se menciona que cuentan con uno.

5 ESTADO DE SITUACIÓN

5.1 INFORMACIÓN PROPORCIONADA AL INTERESADO

Con carácter general y del estudio realizado, se ha observado el estado de situación que a continuación se detalla respecto a la información proporcionada al interesado:

1. Identidad y datos de contacto del responsable y, en su caso, de su representante: todas las empresas analizadas informan sobre la identidad del responsable de tratamiento de los datos personales y proporcionan sus datos de contacto en el apartado dedicado a su política de privacidad. Además, los datos suelen ponerse al pie de las páginas web o bien en su apartado “Aviso legal”. Algunas empresas (grandes) proporcionan información sobre la identidad de todas las filiales del grupo empresarial. No obstante, ninguna de las empresas analizadas proporciona información respecto a la identidad de su representante. En cuanto al modo de contactar con el responsable para cuestiones relativas a la utilización de datos personales, casi todas proporcionan un domicilio postal al cual dirigirse y tres de cada cuatro entidades facilitan una dirección de correo electrónico a tal fin. Por último, se observa que la cuarta parte de las empresas analizadas cuenta con un formulario electrónico habilitado para ello y que proporcionar un número de teléfono de contacto es la excepción entre las entidades analizadas.
2. Contacto del Delegado de Protección de Datos: alrededor de un tercio de las empresas analizadas no cuenta con la figura de un Delegado de Protección de Datos. Cabe señalar que dos de cada tres empresas del sector hotelero analizado no tienen esta figura. En cuanto al modo de ponerse en contacto con él, casi todas las empresas analizadas prefieren proporcionar una dirección de correo electrónico a tal fin. Por último, la tercera parte de las empresas facilita también una dirección de correo postal y solo unas pocas cuentan con un formulario electrónico habilitado para ello.
3. Finalidades del tratamiento: todas las empresas analizadas utilizan los datos personales para la prestación del servicio o producto contratado. Además, casi todas las empresas mencionan entre las finalidades de tratamiento la utilización de los datos para el envío de comunicaciones de carácter comercial. Por su parte, más de la mitad de las empresas revisadas mencionan entre sus finalidades el cumplimiento de obligaciones legales y la prevención del fraude. También, más de la mitad de las empresas utilizan los datos recabados para efectuar perfiles sobre los hábitos de consumo de los usuarios y personalizar los productos ofertados y mejorar el servicio. Y

solo la cuarta parte de las empresas analizadas utiliza los datos para analizar el comportamiento del usuario en el sitio web y mejorar su utilización. Finalmente, solo unas pocas empresas mencionan la utilización de los datos con fines estadísticos. En líneas generales, las finalidades suelen detallarse extensamente, lo cual no siempre redundaba en claridad en la explicación de estas, más bien producen el efecto contrario, ya que un usuario medio es poco probable que lea y comprenda políticas de privacidad que enumeran treinta finalidades distintas de tratamiento de sus datos (como se ha encontrado en algún caso), o bien, que se distingan finalidades según si se ha firmado el contrato o no (como se ha visto en algún caso en que estas finalidades son idénticas o muy similares, por lo que su redacción resulta muy farragosa además de redundante).

4. Base jurídica del tratamiento: de las empresas analizadas, la mitad no detalla la base jurídica del tratamiento como tal. De estas, casi todas enumeran las finalidades para las que se recogen los datos y de ese apartado se infieren o relacionan cuáles son las bases del tratamiento. Por su parte, de las empresas que detallan las bases del tratamiento como tales, la mitad las explica junto con las finalidades de la recogida. Por tanto, del total de empresas analizadas, solo la cuarta parte explica cuál es la base jurídica del tratamiento, en un apartado específico diferenciado. En cuanto a la base jurídica en que se basa el tratamiento, todas las empresas analizadas mencionan el consentimiento del interesado. De estas, casi todas mencionan también la ejecución del contrato con el interesado. Resulta curioso que algunas empresas, del sector hotelero y que utilizan el consentimiento como base jurídica para el tratamiento de datos personales, no mencionen también la necesidad del tratamiento para la ejecución del contrato, cuando resulta evidente que los datos recogidos para efectuar una reserva se apoyan en esta base antes que en el consentimiento. Junto con estas bases jurídicas, dos de cada tres empresas mencionan que el tratamiento es necesario para la satisfacción de intereses legítimos del responsable de tratamiento, mientras que la tercera parte de las empresas analizadas menciona que el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Para finalizar, cabe señalar que, si bien el RGPD reconoce hasta seis bases jurídicas para considerar lícito el tratamiento de datos personales, en el ámbito privado las bases más comunes suelen ser los intereses legítimos del responsable del tratamiento o un tercero (art. 6.1.f) del RGPD), o bien, que el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales (art. 6.1.b del RGPD).

5. Interés legítimo: la gran mayoría de empresas analizadas que menciona el interés legítimo como base para el tratamiento de datos personales detalla de qué intereses se trata. Solo unas pocas hacen una mención genérica al interés legítimo, o bien, aluden al interés de la empresa “*en conocerte mejor y que tu experiencia sea más personalizada*”, sin hacer siquiera referencia al interés legítimo como tal. Entre los intereses enumerados en las políticas de privacidad analizadas, los más comunes son aquellos relativos a la atención al cliente (respuesta a solicitudes, quejas, incidencias). También se menciona como interés de las empresas el análisis de la utilización de la web, a fin de comprobar el comportamiento de los usuarios de la misma, y el envío de comunicaciones comerciales sobre productos o servicios similares a los contratados. En este sentido, cabe recordar que si se trata de la utilización de dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios (*cookies*), o bien, comunicaciones comerciales no solicitadas por vía electrónica o a través de llamadas telefónicas, el régimen jurídico aplicable es el estipulado por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) y la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT), en vez del régimen establecido por el RGPD. Por su parte, también se mencionan como intereses legítimos de los responsables proteger la seguridad de la red y las operaciones, proteger sus derechos y defenderse en caso de disputa, así como la prevención del fraude y otras actividades ilícitas. Por último, se ha observado que varias empresas mencionan entre sus intereses legítimos la realización de perfiles, ya sea para mejorar su oferta de productos y servicios, o bien para prestar un servicio más personalizado al usuario.
6. Destinatarios de los datos recogidos: casi todas las empresas analizadas detallan los destinatarios o categorías de destinatarios de los datos personales recogidos. En general, no lo hacen enumerando todos y cada uno de ellos, sino que más bien se les identifica mediante categorías. En cuanto a los terceros a los que se ceden los datos recogidos, suele tratarse de empresas pertenecientes al mismo grupo empresarial que la entidad analizada, o bien, terceras empresas colaboradoras. En general, se menciona también a las autoridades competentes, tribunales y Administraciones Públicas como destinatarios de la información, cuando sea obligatorio para el responsable. Asimismo, se hace mención a los terceros proveedores de productos o servicios, a los que se facilita la información a fin de cumplir con la prestación contratada. Por último, se observa que unas pocas empresas incluyen el supuesto de ser sucedidas

por otra en su negocio, dentro de las categorías de destinatarios de los datos.

7. Intención del responsable, en su caso, 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 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: del total de empresas analizadas, casi las dos terceras partes mencionan que realizan transferencia internacional de los datos recogidos. En general, se hace mención a aquellas transferencias realizadas fuera del Espacio Económico Europeo (en su mayoría, a EE. UU.) sin detallar las garantías adoptadas. Tan solo se suele hacer una mención genérica, como por ejemplo: *“Siempre que transmitamos información personal a países situados fuera del Espacio Económico Europeo, nos aseguraremos de que la información es transferida de acuerdo con este Aviso de Privacidad y conforme a lo permitido por las leyes aplicables en materia de protección de datos”,* o bien *“...con filiales de la UE y otras entidades de XXX tanto dentro como fuera del Espacio Económico Europeo lo que incluye, entre otros, a XXX con domicilio social en EE.UU., que procesar sus datos personales únicamente de conformidad con nuestras instrucciones y para los fines que se presentan en esta Declaración de Privacidad”* o *“En estos casos, se adoptan las garantías adecuadas para proteger su información”*. Algunas empresas mencionan, entre las garantías, la adopción de cláusulas contractuales tipo o el Escudo de Privacidad entre la Unión Europea y EE. UU. (*“En tales casos, XXXXX garantizará que la transferencia de sus datos personales se realiza de conformidad con las leyes de privacidad aplicables y, en particular, que se apliquen las medidas contractuales, técnicas y organizativas necesarias, como las cláusulas contractuales estándar aprobada por la Comisión Europea”,* o *“A este respecto, le informamos que la misma se encuentra regularizada por medio de cláusulas contractuales tipo, autorizados previamente por la AEPD”,* o bien, *“Entre proveedores se encuentra XXXX, entidad ubicada en Estados Unidos y adherida al Privacy Shield”*). Por su parte, hay que señalar que solo unas pocas empresas analizadas enumeran varios mecanismos que se utilizarán cuando la información sea transferida fuera del Espacio Económico Europeo, tales como cláusulas contractuales tipo aprobadas por la Comisión Europea, el Escudo de Privacidad entre la Unión Europea y los EE. UU., así como normas corporativas vinculantes. Por último, del total de empresas analizadas solo unas pocas incorporan un email a fin de solicitar más información al respecto, y solo algunas mencionan la posibilidad de

conseguir una copia de las garantías adoptadas. Cabe destacar como buena práctica que se ha observado algún supuesto que detalla los destinatarios a los que se transferirán los datos personales, con indicación del país en que se encuentran y el detalle de las medidas adoptadas en cada caso.

8. Información sobre el plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinar ese plazo: del total de empresas analizadas solo unas pocas no hacen referencia al plazo de conservación de los datos personales, mientras que el resto sí que hace alusión a los criterios para determinar dicho plazo. Más de la mitad de estas mencionan que los datos se conservarán mientras exista una obligación legal del responsable del tratamiento y mientras no se solicite su supresión, limitación u oposición. En este sentido, alguna empresa recoge además la solicitud de anonimización de los datos personales, o el derecho a retirar el consentimiento cuando el tratamiento esté legitimado en esta base. También, más de la mitad de las entidades revisadas explican que conservarán los datos personales mientras sean necesarios para cumplir con las finalidades para las que se recogen, o para el cumplimiento de la relación contractual con el usuario. Por su parte, casi la mitad de las empresas estipulan que conservarán los datos recogidos durante el plazo de prescripción de acciones legales que pudieran derivarse. Se ha observado también que algunas empresas hacen referencias un poco genéricas en cuanto a los criterios para determinar el plazo de conservación de los datos, tales como: “*Conservaremos tus datos personales.... mientras no deban eliminarse por ser aún necesarios para XXXXX*”, o “*Los datos recogidos se conservarán mientras exista un interés mutuo*”. Por último, se ha encontrado que unas pocas empresas analizadas detallan el plazo de conservación de los datos personales según la finalidad para la que se utilizan.
9. Derecho a solicitar del responsable 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: todas las empresas analizadas informan sobre los derechos de los interesados. No obstante, unas pocas del sector hotelero enumeran los derechos de los interesados de acuerdo con la anterior normativa aplicable y, por tanto, realizan una enumeración desactualizada. También se ha observado que alguna de las entidades enumera los derechos de los interesados en un apartado dedicado a revocación del consentimiento, en términos como: “*...informándole, a su vez, de que dicho*

consentimiento para que le sean enviadas las mencionadas ofertas comerciales podrá ser revocado en cualquier momento, bastando para ello que dirija carta, o mensaje vía e-mail, indicando el motivo, con firma autógrafa del interesado y fotocopia de su documento nacional de identidad o documento equivalente acreditativo de su identidad, a las direcciones que se indican a continuación, en ejercicio de los derechos de acceso, rectificación, cancelación, oposición, portabilidad y olvido, que como titular de los datos le asisten". Al respecto, cabe señalar que el derecho a retirar el consentimiento otorgado para el tratamiento de sus datos personales (en aquellos casos en que la base jurídica para el tratamiento en cuestión sea la obtención de este consentimiento) es un supuesto distinto al ejercicio por parte de los interesados de sus derechos de acceso a sus datos personales, su rectificación o supresión, o limitación de su tratamiento, u oposición al tratamiento y portabilidad de los datos. En cuanto al procedimiento para el ejercicio de estos derechos, casi todas las empresas lo explican en sus políticas de privacidad junto con la enumeración de derechos con que cuentan los interesados. Respecto al procedimiento previsto, la mitad de las empresas analizadas facilita un domicilio postal y un correo electrónico a tal efecto, mientras que la cuarta parte de las empresas prefiere hacerlo únicamente a través de un formulario electrónico. Por su parte, solo unas pocas empresas además de un formulario electrónico facilitan una dirección de correo electrónico, mientras que otras pocas proporcionan un domicilio postal y un correo electrónico. Hay que señalar que solo de forma excepcional se ponen a disposición los tres medios, tanto un domicilio postal, como un correo electrónico y un formulario electrónico. Del análisis efectuado, se concluye que todas las empresas analizadas proporcionan para el ejercicio de estos derechos al menos un medio electrónico, lo cual resulta adecuado en un entorno como es el *online*.

10. Derecho a presentar una reclamación ante la autoridad de control: casi todas las empresas analizadas sí que cumplen con la obligación de informar sobre el derecho del interesado a presentar una reclamación ante la autoridad de control. Hay que señalar que las pocas empresas que no mencionan este derecho pertenecen al sector hotelero. Todas las entidades que mencionan este derecho indican también ante quién ejercerlo, si bien solo algunas de ellas proporcionan un enlace a la página web de esta Agencia sin más indicación. Dos de cada tres entidades analizadas señalan a la AEPD como la autoridad de control indicada para presentar una reclamación, pero en otras se menciona, por ejemplo, a la Plataforma europea de resolución de conflictos o a "*nuestra autoridad de control principal, la Commission Nationale pour la Protection des Données de*

Luxemburgo o ante un organismo local” o a la Autoridad de protección de datos de Suecia. En cuanto al modo de presentar esta reclamación, más de la mitad de las entidades proporcionan bien un enlace a la página web de la Autoridad de control, o bien un correo electrónico o domicilio postal. Por último, cabe destacar que alguna empresa que menciona a la AEPD lo hace en el apartado “Contacta Con Nosotros” en vez de en aquel donde se detallan las opciones y derechos de los interesados. En cuanto a su redacción, se explica en los siguientes términos: “Si tuvieras cualquier duda o cuestión sobre lo anterior o sobre nuestro enfoque a la privacidad, nuestra Oficina de Privacidad, incluido nuestro Delegado de Protección de Datos, estarán encantados de ayudarte... También puedes acudir a la Agencia de Protección de Datos, si bien te animamos a que primero nos permitas ayudarte”.

11. Información sobre si la comunicación de datos es requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales. En tales casos, posibles consecuencias de no facilitar tales datos: todas las empresas analizadas exigen determinados datos de los interesados para poder contratar su producto o servicio. No obstante, casi la tercera parte no indica que esos datos sean obligatorios en los formularios de recogida, sino que simplemente no permite continuar con el proceso de compra, suscripción o registro. En cuanto a la información sobre las posibles consecuencias de no facilitar tales datos, en general no se ofrece ninguna, solo no se permite continuar con el procedimiento hasta no proporcionar los datos requeridos. No obstante, unas pocas empresas sí que indican que si no se facilitan los datos requeridos no se podrá prestar el servicio que se solicita. Por último, se ha observado que una de cada cinco de las entidades analizadas no especifica en sus apartados dedicados a privacidad que existen datos que son obligatorios o cuya comunicación es un requisito, pero sí que menciona que hay datos que son “necesarios”, sin dar más detalle.
12. Información sobre la existencia de decisiones automatizadas (incluida la elaboración de perfiles) 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: las dos terceras partes de las empresas analizadas reconocen que realizan elaboración de perfiles. La tercera parte restante no hace mención a este tema y, de los datos reflejados en su política de privacidad y avisos legales, no consta que realicen tal actividad. En cuanto a las empresas que realizan elaboración de perfiles, estas no dan al interesado información sobre la lógica aplicada ni

la importancia de estas. En general, esta actividad se menciona entre las actividades de tratamiento realizadas junto con las finalidades para las que se recogen los datos personales. Casi la mitad de estas empresas reconoce la realización de perfiles para mejorar su oferta de productos o personalizar el envío de ofertas comerciales o dar un trato más personalizado al cliente, mientras que un tercio analiza la utilización de su sitio web para comprobar las preferencias y comportamientos de los usuarios. Cabe señalar que alguna empresa en su Política de Privacidad dispone: *“normalmente no adoptamos decisiones automáticas, pero cuando lo hagamos dejaremos claro que se está adoptando ese tipo de decisión”*. No obstante, esta entidad recoge varios apartados dedicados a la personalización de servicios a fin de mostrar publicidad personalizada al ingresar en su sitio web y también para el envío de comunicaciones comerciales personalizadas.

5.2 TRATAMIENTO BASADO EN EL CONSENTIMIENTO DEL INTERESADO

5.2.1 CONSENTIMIENTO INFORMADO

Para que el consentimiento sea informado, es necesario comunicar al interesado ciertos elementos que son cruciales para poder elegir. A tal fin, el Grupo de Trabajo del Artículo 29 sobre Protección de Datos (actual Comité Europeo de Protección de Datos)² ha considerado que se requiere, al menos, la información siguiente para que el consentimiento obtenido sea válido: i) la identidad del responsable del tratamiento; ii) el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento; iii) qué (tipo de) datos van a recogerse y utilizarse; iv) la existencia del derecho a retirar el consentimiento; v) información sobre el uso de los datos para decisiones automatizadas, cuando sea pertinente; y vi) información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas. Respecto al punto primero y a los dos últimos, ya se han analizado en los apartados 1, 12 y 7 del epígrafe 5.1 del presente informe, respectivamente. En cuanto al resto de aspectos de los que debe informarse al solicitar el consentimiento del interesado, con carácter general y del estudio realizado, se ha observado el siguiente estado de situación:

- 13.** Información sobre las categorías de datos que se recogerán y tratarán: la tercera parte de las empresas analizadas no proporcionan información alguna sobre las categorías de datos que se recogerán y tratarán. Como

² Grupo de Trabajo del Artículo 29 sobre Protección De Datos, “Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679” (wp259rev.01): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

curiosidad, cabe mencionar que hay casos que sí que especifican los datos de navegación que se recogerán a través de las cookies del sitio web o que detallan solo los tipos de datos personales obtenidos a través de terceros. Por su parte, alguna empresa tiene en su documento de “Privacidad” un apartado específico dedicado a las categorías y procedencia de los datos personales objeto de tratamiento, pero no se enumeran las categorías de datos tratados, sino solo su procedencia. De las empresas que sí explican los datos que se tratarán, en general no se detallan como parte de la información proporcionada para solicitar el consentimiento de los interesados. Al respecto, se ha encontrado algún caso en que se hace referencia a los datos obtenidos a través de redes sociales en términos como *“que nos la facilitarán en caso de que lo hayas autorizado aceptado sus correspondientes términos y condiciones”*. Cabe destacar que casi la mitad de las entidades que sí explican las categorías de datos que se tratarán, lo hacen de una forma detallada. Por último, se ha observado algún caso que incluye el tratamiento de datos para la gestión de la petición realizada por parte del usuario y explica los datos que se tratarán, pero fundamenta su legitimación en el consentimiento del usuario, cuando, en realidad, se trataría de un tratamiento de datos necesario para la ejecución de un contrato en que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

- 14.** Finalidad(es) para la(s) que se solicita el consentimiento: casi todas las empresas analizadas informan sobre las finalidades para las que se solicita el consentimiento. Más de la mitad de estas dan toda o parte de la información en el mismo formulario de la solicitud de consentimiento, mientras que la tercera parte solo detalla las finalidades en el apartado de Privacidad, al cual se accede a través de un enlace ubicado al final del formulario de recogida de datos. Solo unas pocas de las entidades analizadas informan de todas las finalidades para las que se recogen los datos y solicitan el consentimiento en el formulario de recogida de datos personales. La cuarta parte de las empresas revisadas (pertenecientes al sector del transporte y seguros y que dan algún tipo de información sobre las finalidades del tratamiento en el formulario) decidieron facilitar en el momento de la recogida un resumen de los fines y remitir al usuario al apartado de “Privacidad” para más información. Por su parte, más de la mitad de estas entidades informan solo sobre finalidades vinculadas a comunicaciones comerciales, mientras que el resto de información se concreta en las políticas de privacidad respectivas. En cuanto a las finalidades para las que se solicita el consentimiento, en los apartados de Privacidad suelen detallarse todos los fines del tratamiento de datos

personales que se realiza, sin diferenciar aquellas para las que se solicita el consentimiento del resto de finalidades.

- 15.** Derecho a retirar el consentimiento en cualquier momento: solo unas pocas empresas analizadas (del sector hotelero y del sector seguros) no informan del derecho del interesado a retirar en cualquier momento su consentimiento para el tratamiento de sus datos personales. Por su parte, otras pocas empresas no mencionan este derecho como tal, sino que refieren a que se podrá “*revocar la autorización que dio para tratar sus datos*” o “*el derecho a oponerse a que sus datos personales se procesen para fines de marketing directo*”. Por último, de las entidades que sí informan del derecho a retirar el consentimiento, las dos terceras partes no lo hacen en el formulario por el que se recoge este consentimiento, sino que lo mencionan solo en sus apartados de Privacidad.

5.2.2 SOLICITUD DEL CONSENTIMIENTO

Respecto al modo de obtener el consentimiento del interesado cuando el tratamiento de sus datos está basado en la obtención de este consentimiento, con carácter general y del estudio realizado, se ha observado el estado de situación que a continuación se detalla:

- 16.** Solicitud de consentimiento para cada finalidad de tratamiento: la cuarta parte de las empresas analizadas solicita el consentimiento del interesado para cada finalidad del tratamiento de datos basado en su consentimiento. Del resto, en más de la mitad de los formularios de recogida de datos solo se solicita el consentimiento para el envío de comunicaciones comerciales, mientras que para las demás finalidades se acepta en bloque al aceptar la Política de privacidad correspondiente. En general, suele utilizarse fórmulas del estilo de “*He leído y acepto la Política de privacidad*”, o bien se acepta en bloque varios documentos con la fórmula “*Acepto los términos y condiciones generales, Política de privacidad y condiciones de la reserva*”. En cuanto a la solicitud de consentimiento para el tratamiento de datos con fines publicitarios, cabe señalar que, si se trata de comunicaciones comerciales no solicitadas que se realicen por vía electrónica o a través de llamadas telefónicas, el régimen jurídico aplicable es el estipulado por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) y la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT), las cuales contemplan exenciones y garantías distintas a las previstas por el RGPD. Algunas empresas en una misma solicitud de consentimiento incorporan

varias finalidades, como, por ejemplo: *“Acepto el envío de ofertas comerciales de XXXXX y la realización de un perfil sobre mis hábitos de consumo a través de información interna y externa, tanto durante como tras la finalización de la presente relación contractual”* o *“Acepto el uso de datos para todos los fines detallados en la política de privacidad”*. Por último, cabe reseñar el caso de alguna empresa que menciona en su política de privacidad que se tratarán los datos con fines publicitarios cuando se haya otorgado el consentimiento para ello, pero en el formulario de recogida de datos no hay ninguna opción para darlo.

17. Solicitud de consentimiento a través de un acto afirmativo claro (ni silencio ni casillas premarcadas): la cuarta parte de las empresas analizadas no solicita el consentimiento a través de un acto afirmativo claro. Se trata de entidades que pertenecen tanto al sector hotelero como al sector transporte o comercio electrónico. De estas empresas, más de la mitad no solicitan el consentimiento a través de casilla alguna, sino que aceptan en bloque el tratamiento de sus datos para las finalidades enumeradas en el apartado de Privacidad. Además, se han observado casos en que en el formulario de recogida de datos se permite al usuario marcar una casilla con la leyenda *“No quiero recibir publicidad”*, o bien, que se incluye una casilla premarcada con la leyenda *“Sí, quiero ahorrar dinero recibiendo emails personalizados de XXXX con ofertas increíbles”*. La tercera parte de las entidades que sí solicitan el consentimiento a través de acto afirmativo claro, lo hacen solo para determinados fines (en general, publicidad) mientras que las demás finalidades se aceptan al aceptar la Política de privacidad.
18. Solicitud de consentimiento que se distingue claramente de los demás asuntos: todas las empresas que solicitan el consentimiento del interesado para el tratamiento de sus datos personales lo hacen de forma tal que se distingue claramente de los demás asuntos del formulario de recogida de datos. En general, mediante el marcado de una casilla al final de este formulario.
19. Solicitud de consentimiento que no perturba innecesariamente el uso del servicio: todas las empresas que solicitan el consentimiento del interesado para el tratamiento de sus datos personales lo hacen de forma tal que esta solicitud no perturba innecesariamente el uso del servicio. En general, mediante el marcado de una casilla al final del formulario de recogida de datos personales.

5.3 PRESENTACIÓN DE LA INFORMACIÓN AL INTERESADO

En cuanto a la forma en que se brinda la información al interesado, con carácter general y del estudio realizado, se ha observado el siguiente estado de situación:

20. La información es concisa, transparente, de fácil acceso y con lenguaje claro y sencillo: de las empresas analizadas, alrededor de la mitad no aporta información concisa, más bien al contrario, son documentos largos con muchos apartados, los cuales pueden resultar disuasorios para su lectura por los usuarios. No obstante, todos son de acceso relativamente fácil, dado que en el pie de las páginas web y al final de los formularios de recogida de datos se incluyen enlaces a estos documentos. En cuanto a la forma en que se presenta la información, solo unas pocas empresas no son claras o utilizan un lenguaje difícil. Para finalizar, cabe mencionar algunos casos que resultan llamativos, por ejemplo, incluir la información relativa al tratamiento de datos personales en medio de las condiciones legales para la contratación de sus servicios, o contar con más de una política de privacidad, o mostrar información casi duplicada sobre privacidad, o utilizar una letra demasiado pequeña para leer con comodidad, o tener distintos documentos sobre privacidad según el servicio que se contrate, o detallar en varios documentos todo lo relativo a esta temática.
21. Se facilita la información de forma previa a la recogida de datos: en general, todas las empresas analizadas facilitan la información sobre tratamiento de datos personales de forma previa a su recogida, ya sea mediante un enlace que se facilita a la hora de registrarse o contratar un servicio o producto, o bien a través de un enlace ubicado en el pie de las páginas web. Cabe señalar que más de la tercera parte de las entidades analizadas (la mitad pertenecientes al sector seguros) facilita, en el mismo formulario de recogida de datos, un resumen de la información contenida en su apartado sobre “Privacidad”, con información básica sobre el tratamiento de datos personales que realizan.
22. La información se facilita en capas: en general, las empresas analizadas, en el formulario de recogida de los datos personales, incluyen un párrafo con algo de información sobre su tratamiento e incorporan un enlace a la política de privacidad, con la fórmula “*He leído y acepto la política de privacidad*”. Se ha observado también que unas pocas empresas en su apartado dedicado a “Privacidad” proporcionan información resumida junto con un enlace para luego desplegar la información completa.

23. Medio por el que se ofrece la información: todas las empresas analizadas ofrecen, a través de su página web, la información sobre el tratamiento de datos personales que realizan.

5.4 DELEGADO DE PROTECCIÓN DE DATOS

Con carácter general y del estudio realizado, se ha observado el estado de situación que a continuación se detalla respecto a la figura del Delegado de Protección de Datos:

24. Existencia de un Delegado de Protección de Datos: casi un tercio de las empresas analizadas no cuenta con la figura de un Delegado de Protección de Datos o no informa de ello. Cabe destacar que, en general, todas las grandes empresas sí que lo tienen, mientras que las empresas de menor tamaño son las que no cuentan con uno, si bien no suelen estar obligadas a ello.
25. Denominación con la que se conoce: casi todas las empresas analizadas se refieren a esta figura como “Delegado de Protección de Datos”. Solo menos de la cuarta parte de las páginas revisadas se refieren a ella como “*Oficina de Protección de Datos*”, o bien, “*Responsable de Protección de Datos (DPO)*”. Cabe señalar que unas pocas empresas utilizan dos denominaciones en sus políticas de privacidad y hacen mención a la “*Oficina de Protección de Datos*” y al “*Delegado de Protección de Datos*”.
26. Ubicación de la figura del DPD en la página web: en todas las páginas web donde se informa de esta figura, se menciona en su apartado “Política de privacidad”, al cual se accede desde la parte inferior del sitio web en cuestión. Dentro de este documento, se observa que en general se incluye esta figura dentro del apartado de “Contacto” con la empresa. Por su parte, algunas empresas lo mencionan en el apartado dedicado al “Responsable del tratamiento”.
27. Medio de contacto con el DPD: casi todas las empresas analizadas facilitan una dirección de correo electrónico para contactar con el Delegado de Protección de Datos. Solo alguna entidad en vez de correo electrónico habilita para ello un formulario específico en la web. Por lo demás, casi la mitad de las empresas, además de una dirección de correo electrónico, proporcionan una dirección postal a la cual escribir a tal fin. Hay que reseñar que en unos pocos casos se observa que la dirección postal facilitada es la del responsable del tratamiento, sin indicar si es la misma o no que la del Delegado de Protección de Datos.

28. Descripción de las funciones del DPD: en las dos terceras partes de las webs analizadas sí que se hace mención de la finalidad para la que puede contactarse con el Delegado de Protección de Datos. En general, se dice que se puede contactar con él a fin de resolver dudas sobre la política de privacidad y hacer consultas sobre el tratamiento de datos personales. En unas pocas páginas web se dice que hay que contactar con él para presentar reclamaciones relativas al tratamiento de datos personales, mientras que en alguno de los sitios web revisados se hace referencia a esta figura como a la que hay que dirigir el ejercicio de los derechos reconocidos a los interesados respecto a sus datos personales.

5.5 OBSERVACIONES GENERALES

29. Observaciones relativas al sector transporte: alguna empresa solicita el consentimiento para el tratamiento de datos con fines publicitarios, pero lo menciona como “*cesión de datos*” y no se pide aparte. Por su parte, alguna entidad recoge datos sociodemográficos (como edad, situación familiar, residencias, estudios y ocupación) y no es clara respecto a si elabora o no perfiles de los interesados. Además, menciona que el tratamiento de datos personales se basa en su interés legítimo, pero no especifica cuál es. Por último, alguna empresa prevé el tratamiento de datos para envío de publicidad de terceros sin identificarlos ni indicar sectores de actividad a que pertenecen. Y tampoco informa de modo claro ni la información para el uso de los datos personales para envío de publicidad ni los momentos adecuados para aceptar dicho tratamiento.
30. Observaciones relativas al sector hotelero: se han observado casos en que, si se proporcionan datos de terceros, el usuario “*manifiesta contar con el consentimiento de los mismos y se compromete a trasladarle la información contenida en la Política de Privacidad, eximiendo a XXXXX de cualquier responsabilidad en este sentido*”, o que se indica que para el tratamiento de datos personales del interesado podrá utilizarse información interna y externa proveniente de fuentes accesibles al público. Como curiosidad, se ha encontrado algún supuesto que incorpora pantallas con información sobre el Reglamento Europeo de Protección de Datos en su Aviso Legal (aunque la letra utilizada es muy pequeña, lo cual dificulta su lectura) o que no permite conocer el tiempo de conservación de sus datos, ya que se utiliza una fórmula demasiado genérica (“*mientras exista interés mutuo*”). Por último, también se ha visto algún caso en que no se tiene adaptado el aviso legal al RGPD y se hace referencia a la anterior legislación aplicable, con

muy pocos párrafos, en los que no se proporciona casi información sobre el tratamiento de datos personales.

31. Observaciones sobre el sector de comercio electrónico: unas pocas empresas, al informar sobre los datos personales que se tratan, lo hacen diferenciando los datos facilitados por el usuario, de aquellos obtenidos de forma automática, y de los datos recabados de otras fuentes. alguna empresa, respecto a la publicidad basada en intereses, informa que no se utiliza información que permita identificar a individuos directamente.
32. Observaciones sobre el sector de los seguros: en general, en el formulario por el que se recogen los datos personales y el consentimiento de los interesados para que sus datos sean tratados, se muestra un resumen con los aspectos más relevantes sobre protección de datos personales y se proporciona un enlace al apartado dedicado a “Privacidad” de la página web en cuestión. En cuanto a la forma en que se presenta esta información, unas pocas empresas tienen un documento sobre privacidad para cada tipo de producto (se han observado casos con cinco o nueve documentos sobre privacidad). No obstante, estos documentos suelen ser casi idénticos y con la misma información. En este sentido, cabe señalar también que alguna empresa tiene documentos de privacidad distintos según si ya se ha contratado un seguro con la empresa, o no. En cuanto a la base jurídica que legitima el tratamiento de los datos personales, alguna empresa menciona “*el interés público*” o detalla todas las finalidades para las que se tratan los datos, excepto para los tratamientos basados en el consentimiento del usuario. Como curiosidad, alguna entidad señala que “*podrá comunicar sus datos personales a las siguientes entidades aseguradoras, coaseguradoras y reaseguradoras y administraciones públicas*”, pero no detalla a qué aseguradoras, coaseguradoras y reaseguradas se refiere. Por último, cabe destacar como buena práctica que se ha visto algún caso en que, además de informar sobre los derechos que pueden ejercitar los interesados, se menciona expresamente “*Finalmente, usted tiene derecho a que XXXX, como responsable del tratamiento, le entregue sus datos personales en un formato de uso común y de lectura mecánica y/o a transmitirlos a otro responsable*”.
33. Otras observaciones: se han observado supuestos en que se incluye un documento de privacidad muy extenso que no utiliza capas para mostrar la información, o que no especifica el criterio para determinar el plazo de conservación de los datos personales recogidos o bien, que muestra la información de forma muy clara pero lo que dice no es del todo correcto, ya

que, entre otros ejemplos, se menciona como interés legítimo cuestiones que no lo son.

6 RECOMENDACIONES

6.1 INFORMACIÓN PROPORCIONADA AL INTERESADO

Con carácter general y del estudio ya realizado, se recogen las recomendaciones que a continuación se detallan respecto a la información proporcionada al interesado al recoger sus datos personales:

1. Identidad y datos de contacto del responsable y, en su caso, de su representante: se recomienda incluir siempre esta información al principio del documento o apartado de privacidad correspondiente, a fin de que el usuario pueda encontrar esta información de forma rápida y sencilla. En cuanto al modo de contactar con el responsable del tratamiento, se considera más adecuado facilitar al interesado una dirección de correo electrónico o un formulario electrónico, por tratarse de un entorno *online*.
2. Contacto del Delegado de Protección de Datos: cabe recordar que, en los supuestos detallados en el apartado 1 del artículo 37 del RGPD, resulta obligatorio que el responsable y el encargado del tratamiento designen un Delegado de Protección de Datos. Por tratarse de un entorno *online*, se considera más adecuado facilitar al interesado una dirección de correo electrónico o habilitar un formulario electrónico para contactar con este. También sería recomendable unificar la denominación de esta figura en las políticas de privacidad y utilizar la del RGPD, “Delegado de Protección de Datos”, a fin de evitar confusiones.
3. Finalidades del tratamiento: es obligatorio detallar todas las finalidades para las que se tratan los datos personales de los interesados. No obstante, una enumeración demasiado extensa desalienta su lectura y dificulta su comprensión. Sería recomendable ajustar la extensión de estas explicaciones y agrupar las finalidades por categorías (por ejemplo, prestación del servicio, comunicaciones comerciales, cumplimiento de obligaciones legales, entre otras).
4. Base jurídica del tratamiento: se recomienda diferenciar claramente en la información que se proporciona al interesado, además de las finalidades para las que se realiza el tratamiento de la información, cuál es la base jurídica que legitima cada actividad de tratamiento. Se sugiere que esta información se relacione o se ponga a continuación de la información sobre los fines para los que se realiza el tratamiento. A fin de evitar el efecto

contrario al deseado, se recomienda también ajustar la extensión de estas explicaciones y agrupar las actividades de tratamiento según la base jurídica que las legitima. Además, es importante destacar que la información que se proporcione debe ser correcta. Por tanto, la base sobre la que se informa que legitima el tratamiento de datos debe ser acertada. Esto resulta especialmente relevante para los casos en que la base que legitima el tratamiento de datos personales no encaja en ninguno de los supuestos enumerados en las letras b) a e) del artículo 6.1 del RGPD y resulta preciso que el tratamiento se ampare, bien en la prestación del consentimiento del interesado (art. 6.a) RGPD), o bien que el tratamiento 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”* (art.6.f) RGPD). Mención especial merece el tratamiento de datos para fines de mercadotecnia, publicidad y comunicaciones comerciales. El considerando 47 del RGPD señala que el interés legítimo de un responsable de tratamiento *“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”* y que *“el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo”*. No obstante, cuando las referidas comunicaciones se lleven a cabo por medios electrónicos, antes de acudir a la aplicabilidad del artículo 6.1.f) del RGPD, debe tomarse en consideración la aplicación del artículo 21 de la LSSI, el cual exige que estas comunicaciones hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas, o bien, que *“exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente”*. En cuanto a las acciones de publicidad o mercadotecnia no realizadas a través de medios electrónicos, cabría exceptuar de la necesidad de solicitar el consentimiento del interesado, igualmente, a aquellas comunicaciones relativas a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. Al respecto, hay que señalar que, el tratamiento de datos personales para el envío de comunicaciones comerciales por medios distintos a los electrónicos, siempre que se establezca además un procedimiento sencillo para el ejercicio del derecho de oposición, podría

ampararse en el artículo 6.1.f) del RGPD (interés legítimo) cuando el afectado siguiese siendo cliente de la entidad y los productos o servicios ofertados puedan considerarse “similares” a los contratados por el cliente³.

5. Interés legítimo: cuando el tratamiento de datos esté basado en los intereses legítimos del responsable o de un tercero, debe detallarse cuáles son estos intereses para realizar cada actividad de tratamiento. No basta con hacer una mención genérica al “*interés legítimo*” como tal ni utilizar fórmulas abstractas del tipo “*conocerte mejor*”. Se reitera que la información que se proporcione debe ser correcta y que, por tanto, la base sobre la que se informa que legitima el tratamiento de datos debe ser acertada. Por último, sería deseable que, junto con la información sobre el interés legítimo en que se basa el tratamiento de datos, se documente la ponderación realizada entre este interés del responsable y el derecho de los usuarios a la protección de sus datos personales.
6. Destinatarios de los datos recogidos: en su caso, cuando deba informarse sobre los destinatarios de los datos personales tratados, se recomienda también ajustar la extensión de estas explicaciones y agruparlos por categorías. Si no se comunicaran a terceros los datos personales de los interesados, se considera una buena práctica informar sobre este extremo, a fin de que no permanezcan dudas al respecto.
7. Intención del responsable, en su caso, 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 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: se recomienda prestar especial atención a este apartado ya que se ha observado que no se cumple en su totalidad. El RGPD establece que es obligatorio brindar esta información detallada, en el caso de que se realicen transferencias internacionales. Por tanto, no es suficiente informar de manera genérica sobre que estas transferencias se realizan, sino que también debe decirse si existe o no una decisión de adecuación de la Comisión al respecto y, caso contrario, mencionar las garantías que se proporcionan (sin utilizar fórmulas genéricas del estilo “*garantías adecuadas*” sino, al menos, una enumeración general sin entrar al detalle de cada una) y el procedimiento para obtener una copia de estas o de que se prestaron. Toda esta información no debe ser

³ Informe 0195/2017 del Gabinete Jurídico de la Agencia Española de Protección de Datos.

demasiado extensa de modo que desaliente su lectura, por lo que se recomienda revisar su extensión.

8. Información sobre el plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinar ese plazo: debe darse información clara sobre el plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinar ese plazo. Se sugiere, al menos, proporcionar al interesado una idea aproximada de los plazos que la legislación establece en este sentido, o indicar la normativa aplicable de archivos y documentación al sector del responsable. A fin de determinar los criterios utilizados para determinar el plazo de conservación de los datos personales, no resulta aceptable la utilización de criterios indeterminados tales como “*mientras exista un interés mutuo*”. Se recomienda, por tanto, proporcionar al interesado unos criterios de conservación de sus datos personales que le permitan conocer o calcular, con cierto grado de aproximación a la realidad, durante cuánto tiempo el responsable del tratamiento mantendrá los datos en su poder. Por último, se consideraría una buena práctica que los datos recabados con objeto de la adquisición de un producto se borran una vez finalizado el compromiso de compra adquirido y los plazos relativos a las posibles reclamaciones.
9. Derecho a solicitar del responsable 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: es obligatorio informar a los interesados de todos estos derechos, por lo que las entidades que realicen tratamiento de datos personales deben actualizar la información que proporcionan a los interesados e incorporar los derechos que les asisten y que están detallados en el artículo 13.2.b) del RGPD, en especial los derechos de limitación del tratamiento y portabilidad de los datos. Es recomendable que la información sobre los derechos de los interesados se proporcione en un apartado aparte, identificado claramente como tal, en vez de enumerar mezclados los derechos que se tienen junto con el resto de la información sobre el tratamiento. También sería deseable que, junto con la enumeración de estos derechos, se explique el procedimiento para su ejercicio y se facilite a tal efecto una dirección de correo electrónico o se habilite un formulario electrónico, por tratarse de un entorno *online*. Hay que tener en cuenta que el RGPD contempla la utilización de medios electrónicos para el ejercicio de sus derechos por parte de los interesados, en particular cuando los datos se tratan por medios electrónicos, para lo cual habrá que implantar mecanismos que permitan acreditar la identidad del interesado, la recepción

de su solicitud y de la respuesta que hubiera dado la entidad. A modo de ejemplo, la cláusula informativa sobre el ejercicio de los derechos de los interesados podría estipular: *“Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, ante XXXXXXXX, con domicilio en XXXXXXXXXX o en la dirección de correo electrónico XXXXXXXXXX”*.

10. Derecho a presentar una reclamación ante la autoridad de control: se recomienda informar sobre este derecho junto con el resto de los derechos de que dispone el interesado. También sería recomendable que se especifique que la autoridad de control en España es esta Agencia y se facilite un enlace para su consulta (<https://www.aepd.es/>).
11. Información sobre si la comunicación de datos es requisito legal o contractual, o un requisito necesario para suscribir un contrato, o si el interesado está obligado a facilitar los datos personales. En tales casos, posibles consecuencias de no facilitar tales datos: el RGPD obliga a informar de estos extremos. Debe indicarse si esa información es obligatoria o necesaria para el contrato o si facilitar la información es un requisito legal o contractual. Se recomienda además informar de la base para considerar que facilitar la información es un requisito o una obligación. No se considera suficiente indicar que se trata de “información necesaria” o no indicar nada al respecto. También debe informarse sobre las posibles consecuencias de no proporcionar los datos personales, siendo insuficiente no poder completar la acción deseada si no se facilitan los datos personales solicitados. Se recomienda que esta información se detalle en el documento o apartado relativo a privacidad de la web, aun si en el formulario de recogida de datos se señalan los campos obligatorios con un asterisco y se proporciona información resumida al respecto.
12. Información sobre la existencia de decisiones automatizadas (incluida la elaboración de perfiles) 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: el RGPD es claro sobre la información que debe proporcionarse al interesado cuando se tomen decisiones automatizadas. En cuanto a la elaboración de perfiles, que es una actividad bastante común en el entorno *online*, no es suficiente con informar que estos se realizan, sino que debe explicarse también la lógica aplicada para ello, qué importancia tiene esta actividad para el interesado y las consecuencias que este tratamiento podría tener para él. Se recomienda

que se identifique como tal la realización de perfiles y no se utilicen fórmulas del estilo “*se recogen datos para personalizar tu experiencia*” o “*para conocerte mejor*”. También es recomendable que se distingan claramente cada una de las finalidades para las que se realizan perfiles. En cuanto a la información sobre la lógica aplicada, esta debe ser simple y clara, sin necesidad de una explicación compleja o de facilitar los algoritmos utilizados. Simplemente sería deseable que se facilite una explicación breve y sencilla sobre cómo funciona el procedimiento empleado y las razones para su utilización. Por último, se destaca que es obligatorio informar sobre la importancia y consecuencias que este tratamiento puede tener para el interesado.

6.2 TRATAMIENTO BASADO EN EL CONSENTIMIENTO DEL INTERESADO

6.2.1 CONSENTIMIENTO INFORMADO ⁴

Para que el consentimiento sea informado, es necesario comunicar al interesado ciertos elementos que son cruciales para poder elegir. A tal fin, el Grupo de Trabajo del Artículo 29 sobre Protección de Datos (actual Comité Europeo de Protección de Datos)⁵ ha considerado que se requiere, al menos, la información siguiente para que el consentimiento obtenido sea válido: i) la identidad del responsable del tratamiento; ii) el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento; iii) qué (tipo de) datos van a recogerse y utilizarse; iv) la existencia del derecho a retirar el consentimiento; v) información sobre el uso de los datos para decisiones automatizadas, cuando sea pertinente; y vi) información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas. Respecto al punto primero y a los dos últimos, ya se han efectuado las recomendaciones pertinentes en los apartados 1, 12 y 7 del epígrafe 6.1 del presente informe, respectivamente. En cuanto al resto de aspectos de los que debe informarse al solicitar el consentimiento del interesado, con carácter general y del estudio realizado, se realizan las recomendaciones que a continuación se detallan:

⁴ Para más información y consulta de ejemplos de cláusulas con la información que debe proporcionarse a los interesados, esta Agencia pone a disposición de los ciudadanos la “Guía para el cumplimiento del deber de informar” (<https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf>).

⁵ Grupo de Trabajo del Artículo 29 sobre Protección De Datos, “Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679” (wp259rev.01): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

13. Información sobre las categorías de datos que se recogerán y tratarán: el RGPD dispone que se debe informar al usuario sobre las categorías de datos para cuyo tratamiento se solicita su consentimiento. Se recomienda que esta información se facilite en el mismo formulario en el que se solicita el consentimiento del usuario, aunque sea de forma resumida. En caso de que esta información se comunique además en el documento o apartado de privacidad, sería deseable diferenciar la información sobre aquellos datos que se tratarán en base al consentimiento del usuario del resto de la información facilitada.
14. Finalidad(es) para la(s) que se solicita el consentimiento: el RGPD dispone que se debe informar al usuario sobre las finalidades para las que se solicita el consentimiento. Se recomienda que esta información se proporcione en el mismo formulario en el que se solicita el consentimiento del usuario o que, mejor aún, se facilite un resumen en este y luego se detallen las finalidades en el documento o apartado de privacidad. Sería deseable que se identifique claramente cuáles finalidades de tratamiento de datos requieren consentimiento del usuario en vez de enumerar sin más todas las finalidades para las que se tratarán los datos, sin hacer distinción alguna.
15. Derecho a retirar el consentimiento en cualquier momento: debe informarse al interesado de que tiene este derecho. Se recomienda utilizar para ello la fórmula empleada en el RGPD en vez de referirse a que se podrá “*revocar la autorización que dio*” o el “*derecho a oponerse*” a determinados fines de tratamiento. Se considera una buena práctica que se informe de este derecho en el mismo formulario por el que se solicita el consentimiento del usuario para el tratamiento de sus datos personales. También sería deseable que se explique el procedimiento para ejercitar este derecho y se facilite a tal efecto una dirección de correo electrónico o se habilite un formulario electrónico, por tratarse de un entorno *online*. Se recuerda que debe ser tan fácil retirar el consentimiento como darlo. Es importante destacar que el derecho del interesado a retirar el consentimiento que hubiera dado al tratamiento de sus datos personales es un derecho distinto a los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad de sus datos y, por tanto, es menester que resulte clara esta diferenciación en la información que se proporciona al interesado.

6.2.2 SOLICITUD DEL CONSENTIMIENTO

Con carácter general y del estudio ya realizado, se enumeran las recomendaciones que a continuación se detallan respecto a la forma de obtener el consentimiento del interesado, en caso de que el tratamiento de los datos esté basado en la obtención de este consentimiento:

16. Solicitud de consentimiento para cada finalidad de tratamiento: es importante destacar que debe solicitarse el consentimiento del usuario para todas las actividades de tratamiento que no estén legitimadas en otra base distinta que justifiquen su licitud. Al respecto, se recuerda la importancia de proporcionar información correcta y acertada (ver apartado 4 del epígrafe 6.1 del presente informe). Por su parte, cabe destacar que no resulta apropiado solicitar en bloque el consentimiento del usuario para todas las finalidades de tratamiento de sus datos, sino que debe darse el consentimiento para cada finalidad. A tal fin, se recomienda agrupar en propósitos afines las finalidades para las que se solicita el consentimiento, de forma que el interesado pueda decidir para qué da su consentimiento.
17. Solicitud de consentimiento a través de un acto afirmativo claro (ni silencio ni casillas premarcadas): el RGPD dispone que el consentimiento debe darse mediante un acto afirmativo claro y considera que el silencio, las casillas ya marcadas o la inacción no debe constituir consentimiento. Por tanto, es de obligado cumplimiento que para recabar su consentimiento se facilite al usuario una casilla en blanco o un mecanismo similar. Antes de facilitar sus datos personales y dar su consentimiento al tratamiento de estos, sería deseable que se recomendara al interesado leer y comprender la política de privacidad. Además, se consideraría una buena práctica recordarle al usuario su elección de permisos y solicitar una confirmación de su consentimiento, de la misma forma que muchas veces se pide una segunda confirmación cuando el usuario se da de baja de un servicio *online* o de las comunicaciones publicitarias.
18. Solicitud de consentimiento que se distingue claramente de los demás asuntos: el RGPD exige que la solicitud de consentimiento se distinga claramente de los demás asuntos. A tal fin, se recomienda que el consentimiento se solicite de forma clara, en un apartado específico del formulario por el que se recogen sus datos. Sería deseable que, además, para la solicitud de su consentimiento se utilice una letra más grande o en negrita o color que la diferencie, en vez de usar para ello una letra diminuta o en cursiva que suele pasar desapercibida. Por último, cabe destacar que no se considera suficiente obtener el consentimiento del usuario mediante un botón con una leyenda genérica del estilo “*He leído y acepto las*

condiciones de la política de privacidad” sino que debe distinguirse lo que es consentimiento para el tratamiento de datos personales de lo que es el resto de la relación del interesado con el responsable en cuestión. Se recomienda que la solicitud del consentimiento del interesado incluya opciones para granular y activar el consentimiento y así luego poder marcar la opción *“He leído y acepto las condiciones de la política de privacidad”* o fórmulas equivalentes.

- 19.** Solicitud de consentimiento que no perturba innecesariamente el uso del servicio: tal como se mencionó anteriormente, se recomienda que la solicitud de consentimiento se realice en un apartado específico del formulario por el que recoge los datos, de modo tal que no distraiga la atención del tratamiento de datos personales necesario para la ejecución de la relación que el interesado está contratando. Cabe destacar que no se considera adecuado el uso de ventanas emergentes para solicitar el consentimiento de los interesados para el tratamiento de sus datos personales que obstaculicen la utilización del servicio solicitado.

6.3 PRESENTACIÓN DE LA INFORMACIÓN AL INTERESADO⁶

Finalmente, con carácter general y del estudio ya realizado, se proporcionan las recomendaciones que a continuación se detallan en cuanto a la forma en que se brinda la información al interesado:

- 20.** La información es concisa, transparente, de fácil acceso y con lenguaje claro y sencillo: se recomienda que la información completa relativa al tratamiento de datos personales se facilite en un único documento o en una misma ubicación dentro del sitio web. A tal fin, en el entorno *online* sería una buena práctica la utilización de hipertexto con enlaces para aprovechar las facilidades de organización y presentación de texto que ofrece este sistema, en vez de ofrecer al usuario la información en forma de texto secuencial de principio a fin. Se recomienda también que se utilice un tamaño de letra promedio que no dificulte su lectura y que se organice la información en párrafos o apartados que facilite su comprensión. Es muy importante que se cuide el lenguaje utilizado y no se pierda de vista que el objetivo final es que el usuario pueda tomar decisiones informadas sobre la utilización de sus datos personales. Para ello, se recomienda no usar términos excesivamente técnicos o jurídicos, que no puedan ser

⁶ Para más información sobre cómo proporcionar la información al interesado, la Agencia Española de Protección de Datos pone a disposición de los ciudadanos la “Guía para el cumplimiento del deber de informar” (<https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf>).

comprendidos por un usuario medio, ni resultar en un exceso de información que solo confunda más.

21. Se facilita la información de forma previa a la recogida de datos: se recomienda ofrecer, al menos, un resumen de la información más importante sobre el tratamiento de datos personales, sin remitir a otros documentos o apartados mediante enlaces, de forma previa a que el interesado facilite sus datos y otorgue su consentimiento para su tratamiento. Además, sería deseable que en la parte superior del formulario de recogida de datos se recomendara al interesado leer y comprender el documento o apartado relativo a privacidad antes de facilitar sus datos personales y otorgar el consentimiento para su tratamiento.
22. La información se facilita en capas: se recomienda adoptar un modelo de información por capas o niveles de tal manera que se presente al interesado una información básica reducida y una información adicional más detallada. Se sugiere facilitar como información básica, al menos: identidad del responsable del tratamiento y de su representante (en su caso), finalidad del tratamiento, modo en que el afectado podrá ejercitar los derechos establecidos en los artículos 15 a 22 del RGPD, además de si los datos serán tratados para la elaboración de perfiles (en su caso), en cuyo caso habría que informarle de su derecho a oponerse a la adopción de decisiones individuales automatizadas que pudieran producir efectos jurídicos sobre él o afectarle significativamente. Por último, junto con la información básica debería hacerse una referencia al procedimiento para obtener la información adicional (segunda capa). En un segundo nivel, además de ampliar la información básica, se sugiere incluir base de legitimación del tratamiento, los destinatarios de los datos, la procedencia de los datos si no se hubieran obtenido del interesado, los datos de contacto del Delegado de Protección de Datos (en su caso), los criterios de conservación de los datos, decisiones automatizadas, previsión de transferencias internacionales y el derecho a presentar una reclamación ante las Autoridades de Control. Para estos fines, se recomienda la creación de una estructura de texto que incluya una pantalla inicial con un resumen y apartados desplegables, o bien, enlaces a otras pantallas con los diferentes aspectos de la información (datos tratados y finalidades, derechos, políticas, transferencias internacionales, entre otros), todo lo cual permitiría al usuario acceder a la información más fácilmente y según sus intereses.
23. Medio por el que se ofrece la información: por tratarse de un entorno *online*, se recomienda proporcionar toda la información relativa al tratamiento de datos personales a través de la página web de la entidad en Internet, sin

perjuicio de que se consideraría una buena práctica facilitar también una dirección de correo electrónico o habilitar un formulario electrónico para solicitar más información a este respecto.

6.4 DELEGADO DE PROTECCIÓN DE DATOS

Con carácter general y del estudio ya realizado, se recogen las recomendaciones que a continuación se detallan respecto a la figura del Delegado de Protección de Datos:

24. Existencia de un Delegado de Protección de Datos: de acuerdo con el RGPD, es obligatorio que se designe un Delegado de Protección de Datos en los casos contemplados en el artículo 37.1 (por ejemplo, cuando la actividad principal de la empresa consista en el tratamiento a gran escala de categorías especiales de datos personales). No obstante, sería deseable que, aun en aquellos supuestos en que no resulta preceptiva su designación, las entidades valoren la conveniencia o utilidad de contar con esta figura.
25. Denominación con la que se conoce: sería recomendable unificar la denominación de esta figura en las políticas de privacidad y utilizar la del RGPD en su traducción al español: “Delegado de Protección de Datos”, a fin de homogeneizar la terminología utilizada en estos apartados.
26. Ubicación de la figura del DPD en la web: sería recomendable que la información sobre el Delegado de Protección de Datos se muestre al inicio de la política de privacidad de los sitios web, preferentemente en un apartado específico (no en medio de la información relativa al responsable del tratamiento o en el apartado de contacto con el responsable). Sería de utilidad a los interesados que los datos de contacto del DPD estuvieran, además, en un sitio fácilmente accesible de las páginas web, preferentemente en el apartado de “Contacto” con la empresa o en la sección dedicada a atención al cliente. Por último, se consideraría una buena práctica añadir en el formulario de recogida de los datos personales, junto con un enlace a la política de privacidad, una referencia al modo de contactar con el DPD.
27. Medio de contacto con el DPD: por tratarse de un entorno online, se considera más adecuado, para contactar con el DPD, facilitar al interesado una dirección de correo electrónico o bien habilitar un formulario electrónico en el sitio web a tal efecto.

28. Descripción de las funciones del DPD: sería una buena práctica explicar a los interesados a qué se dedica el DPD y cómo puede serles de utilidad.