0048/2023

La consulta plantea varias cuestiones sobre la adecuación al RGPD y LOPDGDD de determinados tratamientos de datos personales en la contratación y entrega de productos de operadores de telecomunicaciones y de entidades financieras a través de entidades de mensajería y/o paquetería y la consideración que han de tener estas entidades en relación con el tratamiento de datos que se deriva de la prestación de dichos servicios.

Se solicita, partiendo de supuestos de hecho analizados en distintos procedimientos sancionadores resueltos por esta Agencia, si es conforme a la normativa de protección de datos la captura de la imagen del DNI por parte de las entidades de mensajería en distintos supuestos: en la entrega de bienes adquiridos mediante financiación para cumplir la normativa de prevención de blanqueo de capitales; en la entrega de duplicados de tarjetas SIM, y en la entrega de dispositivos móviles.

I

Con carácter previo, hay que señalar, como se ha mencionado, que la consultante parte de supuestos de hecho que se han analizado en procedimientos sancionadores tramitados por la Subdirección General de Inspección de Datos de esta Agencia, - algunos citados de manera expresa y otros de manera indirecta - y que responden a una casuística determinada, sin que, por tanto, el presente informe vaya a examinar lo resuelto en aquellos. Ni se tienen los elementos de juicio suficientes, ni tampoco es una de las funciones de este Gabinete Jurídico.

El objeto del presente informe se centrará en las cuestiones de carácter general que se puedan extraer de la consulta planteada y no de la adecuación de medidas concretas para tratamientos concretos, pues el establecimiento de las mismas es, precisamente, función de los responsables del tratamiento, y en su caso, encargados de tratamiento, de acuerdo con el nuevo modelo de responsabilidad proactiva que se establece en el marco jurídico del RGPD y de la LOPDGDD.

En efecto, la responsabilidad proactiva implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina el cumplimiento

generalizado de las obligaciones en materia de protección de datos. Comprende el análisis, planificación, establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización, -entendidas como el conjunto de directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas, entre otros-, desde la privacidad desde el diseño y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que permitan al responsable demostrar su cumplimiento.

Determinar por este Gabinete Jurídico qué medidas son adecuadas para los tratamientos que cita la consultante o validar las que propone, con la información que aporta y desde la perspectiva de una entidad sancionada, con distintos procedimientos abiertos en la vía administrativa y otros recurridos en vía judicial, resultaría, por un lado, contrario al nuevo modelo que implanta el RGPD en el que el sistema ha pasado de ser reactivo a convertirse en proactivo. “[E]n el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de ≪accountability≫ o ≪responsabilidad proactiva≫ tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y que se recoge en la Exposición de motivos de la LOPDGDD: *la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan*”.

Es decir, solo el responsable del tratamiento conoce bien el contexto en el que ha de aplicar el RGPD, y por tanto, es éste quien debe determinar las medidas más adecuadas en atención al análisis de riesgos para cada tratamiento.

Y, por otro lado, emitir un pronunciamiento como el solicitado por la consultante, lejos de contribuir a la seguridad jurídica, tendría el efecto contrario, pues se podría interpretar como regla general cuestiones que parten y se basan en supuestos de hecho concretos con un marcado componente casuístico y con evidente interés de parte.

II

Dicho lo anterior, procede recordar, por un lado, el criterio general que se ha venido manteniendo por esta Agencia, sobre el uso de la información del

Documento Nacional de Identidad, y por otro el tratamiento de datos que se deriva del cumplimiento de la normativa de prevención de blanqueo de capitales.

Sobre el tratamiento de la información del DNI, en nuestro Informe 7/2023 se recordaban los criterios generales establecidos al efecto:

> *(…)*
>
> *Nos referimos al uso del NIF que coincide con el DNI. Sobre el uso del DNI, el criterio de esta Agencia es que únicamente se ha de someter a tratamiento cuando la norma así lo establezca, resultando excesivo el mismo cuando se pretende únicamente identificar a las personas, ya que el número del DNI es una información especialmente sensible pues su uso indebido o sin las garantías suficientes puede tener múltiples efectos desfavorables para el titular de los datos.*
>
> *En el Informe 88/2020 se analizaba la inclusión del DNI en el certificado electrónico del empleado público en relación con su adecuación al principio de minimización, resaltándose los riesgos que puede tener asociados su uso:*
>
> > *la misma (la disposición adicional séptima* [de la LOPDGDD]*) trata de introducir garantías en el tratamiento del DNI/NIE o equivalente, partiendo de la base de la injerencia que puede suponer en el derecho fundamental a la protección de datos personales que se conozcan conjuntamente el nombre y apellidos y el DNI/NIE de una persona, además del importante riesgo de usurpación de identidad que puede producirse.*
> >
> > *En definitiva, lo que hace el citado precepto es introducir las garantías adecuadas en relación con el tratamiento del DNI/NIE que permitan cumplir con dos de los principios fundamentales de la protección de datos recogidos en el artículo 5 del RGPD (…)*
> >
> > *Y a juicio de esta Agencia, iguales cautelas deben adoptarse cuando se trata de asociar el número del DNI/NIE a los nombres y apellidos de su titular, debiendo evitarse que puedan ser conocidos conjuntamente, fuera de los casos en que sea necesario, el nombre y apellidos junto con el número completo del documento nacional de identidad (o, en su caso, el número de identidad de extranjero, pasaporte o documento equivalente).*
>
> *En el Informe 78/2022 sobre el proyecto de Orden por la que se establece un sistema para la identificación del personal con funciones de*

inspección de sanidad exterior, se aborda el uso del DNI con fines de identificación, cuando existen otros elementos que sirven a tal fin:

> *se puede afirmar que el criterio de esta Agencia sobre el uso del DNI en general, y de los empleados públicos en particular en diferentes contextos es que, salvo que la norma lo prevea expresamente y no existan otros elementos que sirvan para la identificación de la persona en cuestión, el uso del DNI puede resultar excesivo e innecesario para cumplir la finalidad de identificación sobre todo teniendo en cuenta lo indicado en el RGPD en su artículo 87 y la protección que se brinda a este dato personal en la propia LOPDGDD en su disposición adicional séptima.*
>
> *Así, en el proyecto de orden sometido a informe, se establece la creación de un Número de Identificación Profesional que se contendrá en la tarjeta de identificación del personal que realice las funciones de inspección y control, lo que, junto a otros elementos como el nombre y apellidos, y restante información que consta en el artículo 4 de la Orden, hacen que el uso del DNI resulte innecesario y excesivo para cumplir la finalidad de identificar unívocamente al titular de la tarjeta.*

Por lo tanto, si existen otras medidas menos gravosas que cumplen ese fin de identificación, lo recomendable es abstenerse de usarlo.

(…)

Siguiendo con el uso del DNI para la identificación en determinados supuestos, procede citar lo indicado al respecto por el Comité Europeo de Protección de Datos en las Directrices 1/2022, v. 2.0, de 28 de marzo de 2023, que, si bien abordan la identificación para el ejercicio de los derechos previstos en los artículos 15 a 22 del RGPD, resultan especialmente clarificadoras pues recogen el carácter residual que debe revestir este tratamiento como método de identificación atendiendo al riesgo que puede suponer (traducción no oficial):

> *70. Como se ha indicado anteriormente, si el responsable del tratamiento tiene motivos razonables para dudar de la identidad de la persona solicitante, podrá solicitar información adicional o confirmar la identidad del interesado. No obstante, el responsable del tratamiento debe asegurarse al mismo tiempo de que no recoge más datos personales de los necesarios para permitir la identificación de la persona solicitante. Por lo tanto, el responsable del tratamiento llevará a cabo una evaluación de la proporcionalidad, que deberá tener en cuenta el*

tipo de datos personales tratados (por ejemplo, categorías especiales de datos o no), la naturaleza de la solicitud, el contexto en el que se realiza la solicitud, así como cualquier daño que pueda derivarse de una divulgación indebida. Al evaluar la proporcionalidad, debe recordarse que debe evitarse una recopilación excesiva de datos, garantizando al mismo tiempo un nivel adecuado de seguridad del tratamiento.

71. El responsable del tratamiento debe aplicar un procedimiento de autenticación (verificación de la identidad del interesado) para estar seguro de la identidad de las personas que solicitan el acceso a sus datos y garantizar la seguridad del tratamiento durante todo el proceso de tramitación de las solicitudes de acceso de conformidad con el artículo 32, incluido, por ejemplo, un canal seguro para que los interesados proporcionen información adicional. El método utilizado para la autenticación debe ser pertinente, adecuado, proporcionado y respetar el principio de minimización de datos. Si el responsable del tratamiento impone medidas destinadas a identificar al interesado que son gravosas, debe justificarlo adecuadamente y garantizar el cumplimiento de todos los principios fundamentales, incluida la minimización de los datos y la obligación de facilitar el ejercicio de los derechos de los interesados (artículo 12, apartado 2, del RGPD).

(…)

74 Es preciso subrayar que la utilización de una copia de un documento de identidad como parte del proceso de autenticación crea un riesgo para la seguridad de los datos personales y puede dar lugar a un tratamiento no autorizado o ilícito, por lo que debe considerarse inadecuada, salvo que sea estrictamente necesario, adecuado y conforme con el Derecho nacional. En tales casos, los responsables del tratamiento deben disponer de sistemas que garanticen un nivel de seguridad adecuado para mitigar los mayores riesgos para los derechos y libertades del interesado al recibir dichos datos. También es importante tener en cuenta que la identificación mediante un documento de identidad no ayuda necesariamente en el contexto en línea (por ejemplo, con el uso de seudónimos) si la persona interesada no puede aportar ninguna otra prueba, por ejemplo, otras características que coincidan con la cuenta de usuario."

Finalmente indicar, que idéntico criterio se ha seguido en diferentes procedimientos sancionadores (por todos el PS/524/2022) en los que basándose en las citadas Directrices se ha considerado excesivo solicitar la copia del DNI a la hora de identificarse para ejercer determinados derechos en

relación con el contexto especifico del caso, en la medida en que “la reclamada no ha acreditado la proporcionalidad de su petición que puede considerarse excesiva”.

En definitiva, y siguiendo al apartado 76 del ciado Dictamen 1/2022, la información del documento de identidad que no sea necesaria para confirmar la *identidad* del interesado, en el contexto concreto, tal y como por ejemplo, el número del documento, la fotografía, o los datos que se pueden leer por máquina, nos lleva a concluir que la solicitud del DNI con la toma de una copia del mismo sería, en principio, un tratamiento excesivo, y que no puede instaurarse por sistema, sino que habrá que analizar, caso por caso, multitud de aspectos, que van desde la base jurídica que legitima dicho tratamiento, sobre todo si está previsto en la ley, hasta el riesgo de dicho tratamiento teniendo presente el principio de minimización y la proporcionalidad de dicha medida, ya que como nos recuerda el Considerando 39 del RGPD *Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. (…). Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.*

III

En cuanto a la identificación mediante DNI para cumplir la normativa de prevención de blanqueo de capitales, debe indicarse que la consultante parte de un hipotético e inusual supuesto en el que, a diferencia del Procedimiento Sancionador citado (PS/413/2021), realizaría un tratamiento por cuenta de un responsable, es decir, de una entidad financiera y por tanto, uno de los sujetos obligados según la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y no en su condición de operadora de telecomunicaciones y/o suministradora de dispositivos de telefonía.

Es decir, plantea una consulta sobre un tratamiento que no lleva a cabo como responsable del tratamiento, sino que es de un tercero.

A este respecto conviene citar lo indicado en la Instrucción 1/2021 de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia en su apartado Segundo, punto 4:

En ningún caso se emitirán informes sobre consultas que se refieran a tratamientos que estén realizando sujetos distintos del propio consultante, (…).

No obstante lo anterior, en relación con el tratamiento de datos personales derivado de la Ley 10/2010, de 28 de abril, y en cuanto a las obligaciones de identificación procede recordar lo indicado en el Informe 47/2021:

Artículo 3. Identificación formal.

1. Los sujetos obligados identificarán a cuantas personas físicas o jurídicas pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones.

En ningún caso los sujetos obligados mantendrán relaciones de negocio o realizarán operaciones con personas físicas o jurídicas que no hayan sido debidamente identificadas. Queda prohibida, en particular, la apertura, contratación o mantenimiento de cuentas, libretas de ahorro, cajas de seguridad, activos o instrumentos numerados, cifrados, anónimos o con nombres ficticios.

2. Con carácter previo al establecimiento de la relación de negocios o a la ejecución de cualesquiera operaciones, los sujetos obligados comprobarán la identidad de los intervinientes mediante documentos fehacientes. En el supuesto de no poder comprobar la identidad de los intervinientes mediante documentos fehacientes en un primer momento, se podrá contemplar lo establecido en el artículo 12, salvo que existan elementos de riesgo en la operación.

Reglamentariamente se establecerán los documentos que deban reputarse fehacientes a efectos de identificación.

3. En el ámbito del seguro de vida, la comprobación de la identidad del tomador deberá realizarse con carácter previo a la celebración del contrato. La comprobación de la identidad del beneficiario del seguro de vida deberá realizarse en todo caso con carácter previo al pago de la prestación derivada del contrato o al ejercicio de los derechos de rescate, anticipo o pignoración conferidos por la póliza.

Como puede observarse, el citado precepto establece una obligación de identificación, estableciendo, asimismo, la forma en la que se debe proceder a la misma: "mediante documentos fehacientes", remitiéndose a la normativa reglamentaria al objeto de determinar "los documentos que deban reputarse fehacientes".

A este respecto, el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, determina dichos documentos en su artículo 6:

Artículo 6. Documentos fehacientes a efectos de identificación formal.

1. Se considerarán documentos fehacientes, a efectos de identificación formal, los siguientes:

a) Para las personas físicas de nacionalidad española, el Documento Nacional de Identidad.

Para las personas físicas de nacionalidad extranjera, la Tarjeta de Residencia, la Tarjeta de Identidad de Extranjero, el Pasaporte o, en el caso de ciudadanos de la Unión Europea o del Espacio Económico Europeo, el documento, carta o tarjeta oficial de identidad personal expedido por las autoridades de origen. Será asimismo documento válido para la identificación de extranjeros el documento de identidad expedido por el Ministerio de Asuntos Exteriores y de Cooperación para el personal de las representaciones diplomáticas y consulares de terceros países en España.

Excepcionalmente, los sujetos obligados podrán aceptar otros documentos de identidad personal expedidos por una autoridad gubernamental siempre que gocen de las adecuadas garantías de autenticidad e incorporen fotografía del titular.

(…) Por otro lado, el artículo 12 prevé otros medios de identificación, sin perjuicio de que deban obtenerse, igualmente, los correspondientes documentos fehacientes:

Artículo 12. Relaciones de negocio y operaciones no presenciales.

1. Los sujetos obligados podrán establecer relaciones de negocio o ejecutar operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren físicamente presentes, siempre que concurra alguna de las siguientes circunstancias:

> *a) La identidad del cliente quede acreditada mediante la firma electrónica cualificada regulada en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En este caso no será necesaria la obtención de la copia del documento, si*

bien será preceptiva la conservación de los datos de identificación que justifiquen la validez del procedimiento.

b) El primer ingreso proceda de una cuenta a nombre del mismo cliente abierta en una entidad domiciliada en España, en la Unión Europea o en países terceros equivalentes.

c) Se verifiquen los requisitos que se determinen reglamentariamente.

En todo caso, en el plazo de un mes desde el establecimiento de la relación de negocio, los sujetos obligados deberán obtener de estos clientes una copia de los documentos necesarios para practicar la diligencia debida.

Cuando se aprecien discrepancias entre los datos facilitados por el cliente y otra información accesible o en poder del sujeto obligado, será preceptivo proceder a la identificación presencial.

Los sujetos obligados adoptarán medidas adicionales de diligencia debida cuando en el curso de la relación de negocio aprecien riesgos superiores al riesgo promedio.

2. Los sujetos obligados establecerán políticas y procedimientos para afrontar los riesgos específicos asociados con las relaciones de negocio y operaciones no presenciales.

No obstante, el uso de dichos medios queda condicionado al posible riesgo de la operación, tal y como señala el artículo 3 de la LPBCFT. Precisamente, la valoración del riesgo es un elemento central en la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo.

Es decir, el DNI es el método de identificación de las personas físicas, a los efectos de cumplir con las obligaciones de dicha ley. Ahora bien, en las operaciones no presenciales que resulten afectadas por dicha normativa habrá que estar a lo indicado en el artículo 12 de la Ley transcrito en el informe que se acaba de citar, y en todo caso debe tenerse en cuenta el análisis de riesgos asociados a una operación no presencial, tanto desde el punto de vista financiero como desde el punto de vista del riesgo para los derechos y libertades del interesado desde la perspectiva de la protección de datos, de acuerdo con lo indicado en los artículos 24 y 32 del RGPD, que implican el análisis del contexto especifico del tratamiento.

IV

Finalmente, sobre la consideración de las empresas de transporte y mensajería desde su rol como responsable del tratamiento o encargado del tratamiento, debe indicarse que habrá que estar al supuesto de hecho concreto recordando que ambos son conceptos funcionales en relación con un determinado tratamiento. Y con la información y documentación aportada por la consultante no puede establecerse un criterio general, pues tal como se verá a continuación, son muchas las circunstancias que deben tenerse en cuenta.

En efecto, son varios los elementos que han de analizase atendiendo a las circunstancias del caso concreto, como por ejemplo la relación jurídica que se haya establecido entre los sujetos intervinientes y sus concretas obligaciones -es fundamental conocer la relación contractual: objeto, margen de maniobra de las partes, poderes de supervisión del cumplimiento, etc.,..-, así como las obligaciones que puedan venir impuestas por el ordenamiento jurídico para la correcta prestación del servicio, lo que será determinante al objeto de valorar si se actúa en condición de responsable del tratamiento o de encargado del tratamiento.

Así se recoge en el Informe 64/2020 que analiza los distintos servicios que presta Correos como operador postal universal y como empresa de transporte y mensajería:

(…) I

> *Antes de proceder al estudio de la posición que corresponde a los subcontratistas, es preciso determinar las diferentes posiciones jurídicas que, en relación con el tratamiento de datos de carácter personal, puede ostentar Correos, atendiendo a los diferentes servicios que presta. A estos efectos, existen distintos informes de esta Agencia en los que, atendiendo al servicio prestado y a los datos concretos manifestados por la consultante, se ha apreciado la consideración, bien de responsable, bien de encargado, de las empresas de servicios postales, mensajería y paquetería.*
>
> *En este sentido, en el Informe 331/2017, emitido a solicitud de DHL y atendiendo a la normativa entonces vigente, se concluía que las empresas de mensajería ostentaban la condición de responsable del tratamiento de los datos personales que se le ceden (datos del remitente y del destinatario) para hacer llegar el sobre a destino, siendo la base jurídica legitimadora del tratamiento, cuando menos, la establecida en el art. 11.2 c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por cuanto, para el*

desarrollo, cumplimiento y control de la relación jurídica entre el remitente y el consultante, se requiere necesariamente la conexión de dicho tratamiento con los ficheros del propio consultante, que le permitirá llevar a cabo el servicio. Asimismo, atendiendo a lo dispuesto en la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, señalaba que "la ley parece establecer unas obligaciones específicas en materia de protección de datos al operador postal derivadas de los derechos fundamentales en liza, que no casan bien con la figura del encargado del tratamiento".

Por otro lado, en el Informe 49/2004, emitido a solicitud de la Universidad de Valencia de acuerdo con las previsiones de la LOPD, se indicaba que "teniendo en cuenta las circunstancias expuestas en la consulta, en que la consultante facilitaría a la Entidad los datos de los destinatarios de los envíos, limitándose ésta a efectuar los mismos, así como a la realización de las operaciones necesarias para dicha realización, y permitir a la consultante conocer el estado de ejecución de los envíos, podrá considerarse que la Entidad Pública Empresarial Correos y Telégrafos tendría en el presente caso la condición de encargado del tratamiento, (…)"

Más recientemente, en el informe 11/2020, solicitado por Correos y teniendo en cuenta la regulación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en los sucesivo), atendiendo a los datos manifestados por las consultantes y sin tener acceso al contenido de los contratos e instrucciones en virtud de los cuales se materializa dicha prestación de servicios, se concluye que Correos debe considerarse encargado del tratamiento, tanto respecto de aquellas entidades a las que presta el servicio postal como cuando actúa como agente de transporte a través de su filial Correos Express.

Asimismo, el Grupo del artículo 29, en su Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», recogía como ejemplo nº 17 el de la "Externalización de servicios de correo":

"Unos entes privados prestan servicios de correo por cuenta de agencias (públicas); por ejemplo, la correspondencia relativa a los permisos familiares y de maternidad por cuenta de la Agencia Nacional

de la Seguridad Social. En este caso, una autoridad de protección de datos señaló que los entes privados en cuestión debían considerarse encargados del tratamiento dado que su cometido, a pesar de realizarse con un cierto grado de autonomía, se limitaba a sólo una parte de las operaciones de tratamiento necesarias para los fines determinados por el responsable del tratamiento de los datos".

Como puede observarse de los distintos informes emitidos por esta Agencia, son diferentes los supuestos que pueden darse, atendiendo a las circunstancias del caso concreto, la relación jurídica que se haya establecido entre los sujetos intervinientes y sus concretas obligaciones, así como las obligaciones que puedan venir impuestas por el ordenamiento jurídico para la correcta prestación del servicio, lo que será determinante al objeto de valorar si se actúa en condición de responsable del tratamiento o de encargado del tratamiento.

Para ello, es necesario partir de las definiciones que establece el RGPD en su artículo 4:

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

Como ya señalaba el Grupo del artículo 29, en su Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», el concepto de responsable era un concepto funcional dirigido a la asignación de responsabilidades, indicando que "El concepto de «responsable del tratamiento» y su interacción con el concepto de «encargado del tratamiento» desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos y la manera en que los interesados pueden ejercer sus derechos en la práctica. El concepto de responsable del tratamiento de datos también es esencial a la hora de determinar la legislación nacional aplicable y para el ejercicio eficaz

de las tareas de supervisión conferidas a las autoridades de protección de datos".

Asimismo, el citado Dictamen destacaba "las dificultades para poner en práctica las definiciones de la Directiva en un entorno complejo en el que caben muchas situaciones hipotéticas que impliquen la actuación de responsables y encargados del tratamiento, solos o conjuntamente, y con distintos grados de autonomía y responsabilidad" y que "El Grupo reconoce que la aplicación concreta de los conceptos de responsable del tratamiento de datos y encargado del tratamiento de datos se está haciendo cada vez más compleja. Esto se debe ante todo a la creciente complejidad del entorno en el que se usan estos conceptos y, en particular, a una tendencia en aumento, tanto en el sector privado como en el público, hacia una diferenciación organizativa, combinada con el desarrollo de las TIC y la globalización, lo cual puede dar lugar a que se planteen cuestiones nuevas y difíciles y a que, en ocasiones, se vea disminuido el nivel de protección de los interesados".

(…)

Asimismo, partiendo de dicho principio de responsabilidad proactiva, dirigido esencialmente al responsable del tratamiento, y al objeto de reforzar la protección de los afectados, el RGPD ha introducido nuevas obligaciones exigibles no sólo al responsable, sino en determinados supuestos, también al encargado del tratamiento, quien podrá ser sancionado en caso de incumplimiento de las mismas.

(…)

Sin perjuicio de la atribución de obligaciones directas al encargado, las citadas Directrices, partiendo de que los conceptos de responsable y encargado del RGPD no han cambiado en comparación con la Directiva 95/46/CE y que, en general, los criterios sobre cómo atribuir los diferentes roles siguen siendo los mismos (apartado 11), reitera que se trata de conceptos funcionales, que tienen por objeto asignar responsabilidades de acuerdo con los roles reales de las partes (apartado 12), lo que implica que en la mayoría de los supuestos deba atenderse a las circunstancias del caso concreto (case by case) atendiendo a sus actividades reales en lugar de la designación formal de un actor como "responsable" o "encargado" (por ejemplo, en un contrato), así como de conceptos autónomos, cuya interpretación debe realizarse al amparo de la normativa europea sobre protección de datos personales (apartado 13), y teniendo en cuenta (apartado 24) que la necesidad de una evaluación fáctica también significa que el papel de un

responsable del tratamiento no se deriva de la naturaleza de una entidad que está procesando datos sino de sus actividades concretas en un contexto específico, por lo que la misma entidad puede actuar al mismo tiempo como responsable del tratamiento para determinadas operaciones de tratamiento y como encargado para otras, y la calificación como responsable o encargado debe evaluarse con respecto a cada actividad específica de procesamiento de datos.

Partiendo, por tanto, de la posibilidad de ostentar diferente condición respecto a los distintos tratamientos que se realizan por la consultante, será preciso analizar cada uno de ellos atendiendo a las obligaciones legales que le incumben y a las circunstancias del caso concreto, al objeto de determinar si se actúa como responsable o como encargado de tratamiento, pudiendo, al menos, diferenciarse los supuestos que se indican a continuación, diferenciación que se lleva a cabo sin carácter de exhaustividad dada la casuística que puede plantearse.

En primer lugar, deberá atenderse al caso en que el cliente de la consultante sea una persona física que actúa amparada por la denominada "excepción doméstica", en cuyo caso Correos tendrá la consideración de responsable del tratamiento, tal y como se indica en el Considerando 18 del RGPD:

(…)

En segundo lugar, deberá tenerse en cuentas las obligaciones legales que recaen sobre Correos de acuerdo con la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal.

(…). En estos casos, en los que la ley impone obligaciones específicas que implican el tratamiento de datos de carácter personal para la adecuada prestación del servicio y la exigencia, en su caso, de posibles responsabilidades, Correos ostentará la condición de responsable del tratamiento.

Asimismo, Correos debe cumplir con las obligaciones específicas que le corresponden en cuanto operador designado por el Estado para prestar el servicio postal universal cuyo ámbito viene definido por el artículo 21(…)

Por consiguiente, en el ámbito de la prestación del servicio postal universal la capacidad negocial entre Correos y sus clientes respecto a la forma en la que se debe prestar el envío está muy limitada, siendo el legislador nacional el que ha establecido las mismas, lo que en relación

con la normativa de protección de datos implica que los tratamientos se realizan al amparo de lo previsto en las letras 6.1.c) y e) del RGPD, siendo la propia norma la que, al amparo de lo previsto en los apartados 2 y 3 del citado artículo 6, introduce especificaciones respecto al tratamiento de datos personales, delimitando los fines y medios del tratamiento y asignándoselo a Correos que, de este modo, tendrá siempre la consideración de responsable respecto de los tratamientos de datos personales necesarios para prestar el servicio postal universal, de acuerdo con lo previsto en el artículo 4.7) del RGPD in fine.

Por otro lado, como norma especial, en los supuestos en que sea contratado por una entidad sujeta a la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, (…) ostentará la condición de encargado al amparo de lo previsto en su disposición adicional vigesimoquinta: (…)

Por consiguiente, en los supuestos en los que Correos sea contratado de acuerdo con la legislación de contratación del sector público, ostentará la condición de encargado del tratamiento, siempre que no se trate de prestaciones incluidas en el servicio postal universal, en el que, como hemos visto, ostenta la condición de responsable de acuerdo con la Ley 43/2010, la cual establece igualmente obligaciones específicas cuando el servicio se presta al sector público, como ocurre respecto de la práctica de notificaciones administrativas y judiciales a las que se refiere el artículo 22.4 de la misma, que gozarán de la presunción de veracidad y fehaciencia en la distribución, entrega y recepción o rehúse o imposibilidad de entrega, regulando los artículos 39 y siguientes del Real Decreto 1829/1999 los requisitos de dichas notificaciones y los datos personales que deben tratarse.

Por último, en los casos en los que el cliente sea una persona jurídica o una persona física que no se encuentre amparada por la "excepción doméstica" y no se trate del servicio postal universal, podría darse el caso de que Correos actuara como encargado del tratamiento, siempre que concurran en el caso concreto los requisitos necesarios para ello y se haya suscrito el contrato previsto en el artículo 28.3 del RGPD. Esta previsión podría ser aplicable en los supuestos en que exista una relación jurídica previa entre el responsable del tratamiento y el afectado (como, por ejemplo, una compraventa), en los que los datos personales son recabados por el responsable con una finalidad específica (en el supuesto del ejemplo, dar cumplimiento a sus obligaciones como vendedor, entre las que se encuentra la de proceder a la entrega en la

forma pactada entre las partes), decidiendo el responsable el medio a través del cual se va a proceder a dicha entrega, y, por tanto, contratar con Correos la entrega del objeto vendido atendiendo a los datos personales que, a este objeto, le ha facilitado el afectado e impartiendo a Correos las instrucciones precisas para el tratamiento de datos personales previa suscripción del contrato del artículo 28.3. del RGPD, tal y como se indicaba en el Informe 11/2020. Todo ello sin perjuicio de que, al igual que ocurre en todos los supuestos de encargo del tratamiento, Correos tenga la consideración de responsable respecto de los tratamientos que hace de sus propios clientes si contienen datos referidos a personas físicas identificadas o identificables.

(…)

En todo caso, deberá analizarse detenidamente y en profundidad la relación jurídica establecida entre las partes al objeto de identificar quién determina los fines y los medios, para lo que las reiteradamente citadas Directrices del CEPD dan distintos criterios que pueden servir para fijar dichas posiciones, partiendo de que la palabra "determinar" implica ejercer realmente una influencia sobre los fines y medios, para lo que no es óbice que el servicio se defina de una manera específica por el encargado, siempre que al responsable se le presente una descripción detallada y pueda tomar la decisión final sobre la forma en la que se realiza el tratamiento y poder solicitar cambios en caso de ser necesario, sin que el encargado pueda introducir posteriormente modificaciones en los elementos esenciales del tratamiento sin la aprobación del responsable (apartado 28) o que se reconozca un cierto margen de maniobra al encargado para tomar algunas decisiones en relación con el tratamiento (apartado 35) pudiendo dejarse al encargado la toma de decisiones sobre medios no esenciales (apartado 39), de modo que el encargado no deberá tratar los datos de otra manera que no sea de acuerdo con las instrucciones del responsable, sin perjuicio de que dichas instrucciones puedan dejar cierto grado de discreción sobre cómo servir mejor a los intereses del responsable permitiendo al encargado elegir las medidas técnicas y organizativas más adecuadas (apartado 78).

Asimismo, otro criterio a considerar es si la entidad involucrada en el tratamiento no persigue ningún fin propio en relación con el tratamiento, sino que simplemente se le paga por los servicios prestados, ya que en este caso, actuaría, en principio, como encargado más que como responsable (apartado 60).

Por ello, si bien como se señalaba en nuestro Informe 11/2020, la figura del encargado del tratamiento obedece a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, el CEPD recuerda que no todos los proveedores de servicios que procesan datos personales en el curso de la prestación de un servicio es un "encargo" en el sentido del RGPD, ya que no depende de la naturaleza de la entidad que está tratando los datos, sino de sus actividades concretas en un contexto específico, de modo que si el tratamiento no constituye un elemento clave del servicio, el proveedor del servicio puede estar en una posición para determinar de forma independiente los fines y medios de ese procesamiento que se requiere para proporcionar el servicio, en cuyo caso puede ser considerado como un responsable y no como un encargado, y, por el contrario, pero reiterando el CEPD que sigue siendo necesario un análisis caso por caso para determinar el grado de influencia que cada entidad tiene efectivamente para determinar los fines y medios del tratamiento (apartado 80) ya que podrá seguir actuando como encargado incluso si el tratamiento de los datos personales no son el objeto principal del servicio, siempre que el cliente del servicio determine los fines y medios del tratamiento en la práctica (apartado 81).