N/REF: 00148/2019

La consulta plantea la adecuación a la normativa de protección de datos de la guía de plazos máximos de conservación de datos personales que a la misma se acompaña, referida a la actividad de la entidad consultante y elaborada en relación con las diferentes finalidades para las que los datos son recopilados por las diversas entidades que componen su grupo empresarial.

Según se expone por la consultante, en la elaboración de dicha guía se han tenido en cuenta los plazos de conservación derivados de las obligaciones legales y las circunstancias específicas de *la entidad consultante* -identificadas por los responsables del tratamiento de cada entidad dentro del grupo empresarial-, con el objetivo de garantizar la protección de los datos de carácter personal de los afectados.

A su consulta -además de la guía elaborada-, la consultante acompaña un informe sobre justificación de plazos de conservación de documentación, elaborado por el área de Recursos Humanos.

Como cuestión previa, conviene referir que, en el momento de la formulación de la consulta debe partirse del nuevo régimen instaurado por el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, **RGPD**) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -**LOPDGDD**-.

En efecto, como indica la Exposición de motivos de la Ley 3/2018 “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”.

Por consiguiente, es el responsable del tratamiento el que debe cumplir con los principios que se recogen en el artículo 5 del RGPD, entre los que se encuentra, según lo visto, el de responsabilidad proactiva, recogido en su apartado 2, “el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad

proactiva»)". Y entre los principios del apartado 1 se encuentra el de "limitación del plazo de conservación", recogido en su letra e).

A su vez, el artículo 38.1 del RGPD establece claramente que "El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales" y el artículo 39.2 dispone que "El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento".

Finalmente, el artículo 39.1 enumera las funciones del delegado de protección de datos, entre las que se encuentran ""informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros" (apartado a), "supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes" (apartado b) y "ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (apartado c).

Asimismo, le corresponde al delegado de protección de datos "actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto" (apartado e).

En el presente caso es el propio delegado de protección de datos quien plantea la consulta alegando, con carácter general, las dudas que surgen a consecuencia de la aplicación del nuevo régimen jurídico de protección de datos de carácter personal. Así, según señala, solicita el parecer de esta Agencia en aras de la seguridad jurídica necesaria en la realización de sus tratamientos de datos de carácter personal, acompañando a su solicitud el informe emitido por el área de Recursos Humanos respecto a determinados tratamientos incluidos en la Guía, pero sin aportar su propio informe ni razonar cuáles son las dudas que se suscitan y que puedan tener un alcance general, pretendiendo con su consulta la validación, por parte de esta Agencia, de la Guía elaborada, lo que excede de las competencias propias de una autoridad de control y no se corresponde con el principio de responsabilidad proactiva introducido por el RGPD.

En este punto, conviene recordar que son numerosos los informes emitidos por esta Agencia referidos a las previsiones del artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, cuyo apartado 5 se refería a la conservación de los datos y su apartado 3 a la obligación de bloqueo.

En este sentido, nuestro informe de 30 de julio de 2004, reiterado en otros muchos, señalaba lo siguiente:

> "(...) la Ley Orgánica 15/1999 viene regular el bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que "la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".
>
> Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que indica que "los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".
>
> Del análisis conjunto de las normas citadas se desprende que existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado.
>
> Así, el artículo 16.3 viene a reconocer, en consonancia con lo previsto en el artículo 16.5 de la Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley, impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.
>
> Por el contrario, el responsable del fichero estará obligado, bien por el contenido de aquélla relación jurídica, bien por lo establecido en

una norma imperativa, al mantenimiento del dato, si bien sometido a determinadas condiciones que aseguren y garanticen el derecho del afectado a la protección de sus datos de carácter personal, no pudiendo disponer de tales datos en la misma medida en que podría hacerlo en caso de que no procediera (de oficio –por haber dejado de ser necesarios para el cumplimiento de la finalidad del fichero- o a solicitud del afectado) la cancelación de los mismos.

En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto “en las disposiciones aplicables” o a la “atención de las posibles responsabilidades nacidas del tratamiento”, tal y como prevé la meritada Ley.

En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En todo caso, debe recordarse que el mantenimiento del dato bloqueado, supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que “cumplido el citado plazo deberá procederse a la supresión).

En consecuencia, a nuestro juicio, la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.

En lo atinente a la determinación de los períodos en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave.

Por último, en cuanto al modo de llevar a cabo el bloqueo, deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de una requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia."

Por consiguiente, partiendo de lo señalado anteriormente, el presente informe se limitará analizar, desde una perspectiva general, las novedades introducidas por el RGPD en relación con el principio de limitación del plazo de conservación y las previsiones al respecto de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, pero sin realizar una enumeración taxativa de los diferentes supuestos que pueden darse ni un análisis exhaustivo de la Guía remitida, al ser una obligación que corresponde al responsable del tratamiento y exceder de las funciones de asesoramiento por parte de esta Agencia.

I

La consultante se refiere a sus obligaciones en materia de conservación, supresión y bloqueo de la información con datos de carácter personal, derivadas tanto de su actividad mercantil, como de su gestión interna -especialmente, la relativa a recursos humanos-, planteando una propuesta concreta en relación con dicha conservación y bloqueo de los datos que, de acuerdo con el informe que acompaña, vincula a los plazos de prescripción de las correspondientes acciones en el ámbito civil, mercantil y/o laboral.

Bajo la denominación de principio de *"limitación de plazo de conservación"*, el Reglamento general de protección de datos se refiere a la conservación de los datos personales en su artículo 5 letra e), según el cual los datos serán "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento

de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado."

Además, de acuerdo con los principios de *"minimización de datos"* y de *"exactitud"*, recogidos -respectivamente- en las letras c) y d) del citado artículo 5 del RGPD, dichos datos serán "c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" y d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".

De estas últimas exigencias deriva la necesidad de complementar las disposiciones normativas relativas a conservación, minimización y exactitud de datos, con las relativas a los *derechos de los afectados* por los tratamientos, y, en especial, con el derecho de supresión, recogido en el artículo 17 del RGPD, que tiene por objeto *la eliminación* –sin dilación indebida- de los datos personales cuando concurra alguno de los *supuestos* que en dicho precepto se regulan, constituyendo la causa principal la desaparición de la finalidad que motivó el tratamiento para el que los datos fueron recogidos.

No obstante, hay excepciones en las que es posible mantener y tratar los datos por más tiempo del necesario para la consecución de la finalidad originariamente perseguida. Así, los artículos 5.1, letras b) y e), y el propio artículo 17 del RGPD, mencionan -por vía de excepción- los casos de tratamientos ulteriores con fines de archivística en interés público, investigación científica e histórica y fines estadísticos, con las garantías recogidas en su artículo 89. Asimismo, entre otras excepciones que interesa destacar en este momento, se encuentran las contempladas en el apartado 3 del artículo 17 en sus letras b) (cuando el tratamiento sea necesario para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable) y e) (cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones).

Por su parte, el artículo 32 de la LOPDGDD regula la obligación de bloqueo de los datos de carácter personal.

El deber de bloqueo opera tanto en los supuestos de ejercicio de los derechos de rectificación y supresión previstos en el RGPD, como en los supuestos en los que deba procederse de oficio a la supresión de los datos de

carácter personal como consecuencia de la aplicación de los principios establecidos en el artículo 5 del propio Reglamento (UE) 2016/679, de 27 de abril de 2016, tal y como suceder en el caso de que se haya cumplido el plazo de conservación de los datos o que el responsable aprecie que dichos datos no deben ya ser objeto de tratamiento o no debieron serlo incluso con anterioridad.

El bloqueo *excluye el borrado material* de los datos, si bien con las limitaciones que el propio artículo 32 establece.

Se trata así de garantizar la adecuada aplicación y supervisión del cumplimiento de las normas de protección de datos, de forma que sea posible la comprobación de los tratamientos que no resulten conformes con el RGPD y la LOPDGDD, evitando una interpretación extensiva de los plazos de conservación de los datos personales, que no deberán ser objeto de tratamiento más allá de lo estrictamente necesario y de conformidad con las reglas de supresión previstas en estas normas.

Por este motivo, el artículo 32.2 de la Ley Orgánica 3/2018, de 5 de diciembre, establece el alcance de la obligación de bloqueo, al disponer la prohibición del tratamiento de estos datos excepto para su puesta a disposición de los jueces y tribunales, del Ministerio Fiscal o las Administraciones Públicas competentes -en particular de las autoridades de protección de datos-, y para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. A su vez, el artículo 32.3, prohíbe cualquier otro tratamiento de los datos para fines distintos de los citados.

En todo caso, el artículo 32.5 prevé la posibilidad de que las autoridades de protección de datos establezcan excepciones a la obligación de bloqueo en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

II

La *conservación* de los datos de carácter personal y la eventual *supresión* de su tratamiento -bien por imperativo del principio de *"limitación del plazo de conservación"*, o bien como consecuencia del ejercicio del derecho de supresión por los afectados-, se encuentra directamente vinculada con la *finalidad* para la que los datos fueron recogidos y tratados por la entidad consultante. Así, de acuerdo con el artículo 5.1 b) del RGPD, los datos personales deben recogerse con *fines determinados, explícitos y legítimos*, y no deben ser tratados ulteriormente de manera incompatible con dichos fines –"principio de limitación de la finalidad"-.

Además, el análisis de los datos personales, -no ya de la finalidad- aporta otro supuesto de supresión. Los datos de carácter personal serán suprimidos cuando *hayan dejado de ser exactos y completos* (art. 5.1 d. RGPD). A pesar de que se mantenga viva la finalidad para la cual se realiza el tratamiento, si el responsable no es capaz de mantener los datos actualizados de forma que respondan con veracidad a la situación real de las personas afectadas, estará obligado a suprimir esta información personal. Como es natural, también procede la supresión cuando se esté produciendo un tratamiento contrario a la normativa sobre protección de datos.

Por otra parte, debe recordarse que el considerando 45 del Reglamento (UE) 2016/679, de 27 de abril de 2016, señala la posibilidad de que la finalidad del tratamiento se establezca en virtud del Derecho de la Unión o de los Estados miembros, que, en su caso, determine -entre otras circunstancias- *el plazo de conservación de los datos* y otras medidas para garantizar un tratamiento lícito y leal.

Específicamente, en relación con el encargado del tratamiento, el artículo 33.3 de la LOPDGDD, incorpora una regla especial vinculada a la finalización de la prestación de los servicios del encargado al responsable, prohibiendo la destrucción de los datos cuando exista una previsión legal que *obligue a su conservación*, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista. Y, el apartado 4 del referido artículo 33, prevé -incluso- la posibilidad de que el encargado del tratamiento conserve debidamente bloqueados los datos, en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Estas especialidades se cohonestan con el artículo 28.3. g) del RGPD, que -al regular el contrato o acto jurídico en virtud del cual se opera el encargo del tratamiento- establece la posibilidad de que, a la finalización de la prestación de los servicios de tratamiento, se conserven los datos personales cuando así se disponga en el Derecho de la Unión o de los Estados miembros.

A su vez, la finalidad debe vincularse a las bases jurídicas que legitiman el tratamiento de datos personales reguladas por el artículo 6.1 del RGPD. Del análisis de los diversos supuestos a los que se referirá este informe, se infiere que, con carácter general, los datos se recaban y tratan para (i) la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales *-letra b-*, o bien, dicho tratamiento resulta necesario (ii) para el cumplimiento de una obligación legal aplicable al responsable del tratamiento *-letra c-*. Sin embargo, según se observa, en algunos supuestos, la base legitimadora de los tratamientos de la consultante podría encontrarse también (iii) en el consentimiento del interesado *-letra a-*, (iv) en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero *-letra f-,* e incluso (v) en la necesidad de proteger intereses vitales del interesado *-letra d-*.

Por todo ello, solamente será posible la conservación de los datos para los fines establecidos para las *actividades de tratamiento* de la mercantil consultante, vinculados a las finalidades para la que los datos fueron recogidos y tratados por dicha entidad *-ex artículo 5.1 b) RGPD-,* y en tanto concurran las bases jurídicas que justifican la realización de los correspondientes tratamientos *-ex artículo 6.1 RGPD-.*

En este escenario, corresponde al *responsable* del tratamiento -que es el que ha determinado su finalidad- decidir cuándo los datos han dejado de ser necesarios para la finalidad para la cual fueron recabados -decayendo la posibilidad de su tratamiento-, si bien, en algunas ocasiones, es el legislador quien fija un plazo de conservación determinado en relación con supuestos o materias concretas.

Así, siguiendo en este punto el Considerando (39) del RGPD:

> "(39) (…) En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que *se limite a un mínimo estricto su plazo de conservación.* Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales *no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.* Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

En idéntico sentido, el apartado f) del artículo 30 RGPD, al regular el *"Registro de las actividades de tratamiento",* establece que en este se deberán contener, cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

III

Como se ha adelantado, el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, configura el *"bloqueo de los datos"* como una *obligación de responsabilidad activa.* Se establece así que el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o *supresión.*

En consecuencia, la supresión da lugar al bloqueo de los datos, lo que impide el tratamiento para la finalidad que justificó su recogida, conservándose únicamente *(i)* para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, **y** *(ii)* para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de estas -*ex artículo 32.2 LOPDGDD-.*

La interpretación teleológica de este precepto apunta a la consideración de una única posibilidad -*y no de dos*-, en relación con la concurrencia de los requisitos que justifican *este bloqueo*. Así, de una parte, *(i)* la mención de los posibles sujetos -eventuales cesionarios de los datos bloqueados-, y, de otra parte, *(ii)* la referencia al supuesto fáctico -exigencia de posibles responsabilidades derivadas del tratamiento- en cuya virtud los datos bloqueados podrían ser *puestos a su disposición*, constituyen requisitos acumulativos. Finalmente, el artículo 32.2 contiene una referencia expresa a la necesaria consideración del plazo de prescripción de las responsabilidades, que debe interpretarse como plazo de prescripción de las acciones encaminadas a su exigencia.

Esta interpretación se cohonesta con las previsiones que -con anterioridad a la entrada en vigor del RGPD y de la LOPDGDD-, se contenían en los artículos 16.3. de la Ley Orgánica 15/1999, de 13 de diciembre -LOPD-, y en su reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

En concreto, en el artículo 16.3 de la LOPD se señala que:

> "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas."

Y en el artículo 5.1 b) de su reglamento de desarrollo -referido a *Definiciones*- se dispone que:

> "b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos."

En similar sentido, el Consejo de Estado, en su Dictamen 757/2017, de 26 de octubre de 2017, emitido en relación con el anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, después de analizar la

estrecha relación existente entre el bloqueo de los datos y el ejercicio de los derechos de los afectados reconocidos por el RGPD, señala:

> "Sin embargo, a juicio del Consejo de Estado, la cuestión ha de abordarse desde una perspectiva diferente, a la que apunta su nueva ubicación en el texto proyectado. El bloqueo de datos no se configura -y no debe configurarse- como un derecho de los interesados, sino como una obligación del responsable. Su razón de ser radica, como se ha apuntado, en la garantía de una adecuada aplicación y supervisión del cumplimiento de las normas de protección de datos. Así, la efectividad de las previsiones del Reglamento Europeo está vinculada a la exigencia de que se impongan -en caso de incumplimiento- sanciones efectivas, proporcionadas y disuasorias; y el Reglamento Europeo sí incluye una habilitación específica a los Estados miembros, o incluso un mandato, al disponer que "adoptarán todas las medidas necesarias para garantizar su observancia" (artículo 84 del Reglamento Europeo). En la misma línea, la previsión de este artículo 33 ha de ponerse en relación con el derecho a la tutela judicial "efectiva" a que se refieren los artículos 78 y 79 del Reglamento Europeo; como también con la efectividad del derecho a indemnización y responsabilidad que contempla su artículo 82.
>
> En suma, difícilmente puede garantizarse el cumplimiento efectivo de las normas del Reglamento Europeo (y los derechos a la tutela judicial efectiva y a indemnización) si no se impone, en los casos necesarios, el bloqueo de los datos y su puesta a disposición de los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes "para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas".

La configuración del *bloqueo de los datos* como una *obligación de responsabilidad activa* no obsta, sin embargo, a la utilización por parte del responsable del tratamiento de su derecho de defensa *-ex art. 24 Constitución Española-*, pero dicha circunstancia solo justifica el acceso del responsable a los datos bloqueados en los estrictos términos del artículo 32 RGPD, por cuanto -según prevé su apartado 3-, los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señaladas en dicho precepto.

El bloqueo consiste en *"la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización (…)"*, y supone, en la práctica, la adopción de dichas medidas y la reducción al mínimo las personas que pueden acceder a la información necesaria para la atención de las mencionadas responsabilidades, debiendo limitarse este acceso a personas con la responsabilidad de contestar las distintas reclamaciones y en virtud del requerimiento judicial o administrativo correspondiente.

Finalizado dicho plazo, deberá procederse a la destrucción *(borrado)* de los datos, no pudiendo ser tratados los datos bloqueados para ninguna finalidad distinta de las señaladas *-ex artículo 32, apartados 2 y 3 RGPD-*.

Por otra parte, existirán determinados supuestos en los que la conservación de los datos personales vendrá determinada por la propia normativa legal aplicable. Así, por vía de excepción, el apartado 3, letra b), del artículo 17 del Reglamento General de Protección de Datos, excluye del derecho de supresión, y, en consecuencia, habilita la conservación de los datos de carácter personal objeto de tratamiento en aquéllos supuestos en los que hayan de mantenerse para el debido cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento .

Por ende, en los supuestos en los que la conservación de los datos viene impuesta por la ley especial, no procede el derecho de supresión conforme al artículo 17.3.b) del RGPD anteriormente citado, ni, por ende, el bloqueo de los mismos, sin perjuicio de la obligación del responsable de respetar los principios recogidos en el artículo 5 del RGPD y, singularmente, los de limitación de la finalidad, minimización e integridad y confidencialidad, tal y como se analizará posteriormente al tratar sobre las obligaciones impuestas por la normativa de prevención de riesgos laborales.

En este sentido se ha pronunciado el informe de esta Agencia número 1/2019, relativo a las obligaciones de conservación impuestas por la normativa sobre prevención del blanqueo de capitales y financiación del terrorismo:

> El art. 5.1, letra e) RGPD, dentro de los principios relativos al tratamiento, determina que los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
>
> No se plantea aquí una cuestión de conservación con fines de archivo o para fines científicos, por lo que el principio citado obliga al responsable del tratamiento a conservar dichos datos durante no más tiempo del necesario para las finalidades para los que se recogieron.
>
> De manera concordante con este principio, el art. 17 RGPD otorga a los interesados un derecho de supresión de sus datos personales, y correspondiente obligación para responsable de suprimir dichos datos, entre otras circunstancias cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo el (letra b). Sin embargo, el propio RGPD prevé

que dicho derecho puede tener limitaciones. El art. 17.3 RGPD establece que los apartados 1 y 2 [esto es, no habrá lugar a la supresión] no se aplicarán cuando el tratamiento sea necesario: b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

En interpretación de este apartado, el Considerando 65 RGPD dice así:

(…) En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. (…) Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

En estos casos, la retención ulterior de dichos datos es lícita, dice el RGPD. Esto es, no concurriría un derecho del interesado a la supresión de los datos personales.

El art. 25 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, tras la redacción dada por el Real Decreto-ley 11/2018, de 31 de agosto, establece:

Artículo 25. Conservación de documentos.

1. Los sujetos obligados conservarán durante un período de diez años la documentación en que se formalice el cumplimiento de las obligaciones establecidas en la presente ley, procediendo tras el mismo a su eliminación. Transcurridos cinco años desde la terminación de la relación de negocios o la ejecución de la operación ocasional, la documentación conservada únicamente será accesible por los órganos de control interno del sujeto obligado, con inclusión de las unidades técnicas de prevención, y, en su caso, aquellos encargados de su defensa legal.

En particular, los sujetos obligados conservarán para su uso en toda investigación o análisis, en materia de posibles casos de blanqueo de capitales o de financiación del terrorismo, por parte del Servicio Ejecutivo de la Comisión o de cualquier otra autoridad legalmente competente:

a) Copia de los documentos exigibles en aplicación de las medidas de diligencia debida, durante un periodo de diez años desde la terminación de la relación de negocios o la ejecución de la operación.

b) Original o copia con fuerza probatoria de los documentos o registros que acrediten adecuadamente las operaciones, los intervinientes en las mismas y las relaciones de negocio, durante un periodo de diez años desde la ejecución de la operación o la terminación de la relación de negocios.

2. Los sujetos obligados, con las excepciones que se determinen reglamentariamente, almacenarán las copias de los documentos de identificación a que se refiere el artículo 3.2 en soportes ópticos, magnéticos o electrónicos que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación y su adecuada conservación y localización.

En todo caso, el sistema de archivo de los sujetos obligados deberá asegurar la adecuada gestión y disponibilidad de la documentación, tanto a efectos de control interno, como de atención en tiempo y forma a los requerimientos de las autoridades.

Esto es, impone a los sujetos obligados una obligación de conservación de determinados datos y documentos durante unos determinados plazos de tiempo. Esta obligación legal de conservación de documentos y las finalidades a las que sujeta su uso tras el plazo de cinco años a que se refiere el precepto determinan que el derecho de supresión del interesado se vea aquí desplazado por la ley.

Esto es, por otra parte, lo que establece el art. 32 de dicha ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, con relación a la protección de datos personales.

Artículo 32. Protección de datos de carácter personal.
(….)

3. En virtud de lo dispuesto en el artículo 24.1, y en relación con las obligaciones a las que se refiere el apartado anterior, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 5 de la Ley Orgánica 15/1999.

Asimismo, no serán de aplicación a los ficheros y tratamientos a los que se refiere este precepto las normas contenidas en la citada Ley Orgánica referidas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición. En caso de ejercicio de los citados derechos

por el interesado, los sujetos obligados se limitarán a ponerle de manifiesto lo dispuesto en este artículo.

Lo dispuesto en el presente apartado será igualmente aplicable a los ficheros creados y gestionados por el Servicio Ejecutivo de la Comisión para el cumplimiento de las funciones que le otorga esta Ley.
(…)

En definitiva, la propia ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, exceptúa el derecho del interesado a la supresión de sus datos personales en ese contexto.

Por lo tanto, cabe concluir que la obligación legal impuesta a los sujetos obligados por la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo, de conservación de la documentación a que la ley 10/2010 hace referencia supone un tratamiento necesario para el cumplimiento de una obligación legal que cabe incluir dentro de la excepción al derecho de supresión previsto en el art. 17.3, letra b) del RGPD.

Ahora bien, esta excepción al derecho del interesado a la supresión de sus datos personales no supone ni mucho menos una excepción a que el sujeto obligado (la entidad financiera) debe de tratar los datos personales de conformidad con la normativa de protección de datos (véase el art. 32.1 de la propia ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo), por lo que seguirán siendo de aplicación los principios relativos al tratamiento previstos en el artículo 5 del RGPD, y entre ellos el principio de limitación de la finalidad (letra b); y sobre todo el principio de integridad y confidencialidad (letra f), que determina que dichos datos personales deberán ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

En definitiva, dado que el art. 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que el bloqueo es una obligación impuesta a los responsables del tratamiento cuando proceda la supresión de los datos, no procediendo en este caso, como se ha expuesto, la supresión de los datos, el bloqueo no puede ser considerado base jurídica suficiente para el mantenimiento de los datos por el responsable. Y ello, se añade para finalizar, sin perjuicio de que puedan adoptarse por el responsable del tratamiento aquellas medidas incluidas en la definición o descripción del bloqueo que se contiene en dicho artículo 32 como

medidas técnicas y organizativas para la protección de los datos personales siempre que, ciertamente, dichas medidas no impidan los tratamientos que por obligación legal de la legislación de prevención de blanqueo de capitales se imponen a los sujetos obligados.

IV

Como primera conclusión, el estudio anterior arroja la necesidad de que por la entidad consultante (responsabilidad proactiva) se proceda al *examen* pormenorizado de todos y cada uno de los tratamientos incorporados a su registro de "actividades de tratamiento", determinando para cada uno de los supuestos planteados el plazo concreto durante el cual los datos deberán mantenerse bloqueados como estadio previo a su destrucción y borrado físico.

Prima facie, en relación con dicho análisis, la consultante deberá considerar que para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de *reserva de Ley* en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del *artículo 16.3 de la LOPD*) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado.

Pues bien, en su consulta, la entidad consultante se refiere explícitamente a una amplia variedad de supuestos, que devendrían en habilitaciones concretas en orden al bloqueo de los datos de carácter personal objeto de tratamiento, aludiendo a la concurrencia de diferentes habilitaciones legales que -de acuerdo con su análisis- soportarían el correspondiente juicio de necesidad.

Sin embargo, en nuestra opinión, los diferentes plazos a los que la consultante refiere la *necesidad del bloqueo* de los datos personales -en función de las diversas normas jurídicas e informes internos a los que se refiere su análisis-, *exceden en mucho de las exigencias* derivadas de la normativa aplicable.

Así, al margen del ejercicio de sus derechos por los interesados, reconocidos en los artículos 15 a 22 del RGPD, y sin ánimo de exhaustividad, toda vez que resulta imposible establecer una enumeración taxativa de todos los supuestos objeto de análisis, procede formular las siguientes observaciones.

En relación con las *obligaciones personales*, el punto de partida se sitúa en el plazo de prescripción fijado en el artículo 1964, apartado 2, del Código Civil, al que la consultante deberá atenderse en relación con el bloqueo de datos personales relacionados con dichas obligaciones.

En los informes que -con anterioridad a 2015-, venía emitiendo la Agencia, se hacía referencia al plazo de quince años establecido por dicho precepto hasta su modificación, operada en virtud de la Disposición final primera de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que vino a reducir dicho plazo de prescripción, fijándolo en cinco años, señalando que:

> "Las acciones personales que no tengan plazo especial prescriben a los cinco años desde que pueda exigirse el cumplimiento de la obligación. En las obligaciones continuadas de hacer o no hacer, el plazo comenzará cada vez que se incumplan."

En consecuencia -sin perjuicio del *régimen transitorio* aplicable-, el plazo de prescripción para este tipo de acciones pasó de 15 a 5 años y, por tanto, durante este plazo de 5 años, los datos suprimidos deberán ser bloqueados en los términos previstos por el artículo 32 de la LOPDGDD.

En cuanto a la interpretación que deba darse a este precepto, ha de señalarse que no es competencia de esta Agencia la interpretación de cuestiones tales como el *régimen transitorio* para la aplicación a las acciones personales nacidas antes de la entrada en vigor de esta Ley, más allá de lo indicado en propia Disposición transitoria quinta de la Ley 42/2015, de 5 de octubre, sobre el Régimen de prescripción aplicable a las relaciones ya existentes en materia Civil, que establece expresamente que el tiempo de prescripción de las acciones personales que no tengan señalado término especial de prescripción, nacidas antes de la fecha de entrada en vigor de esta Ley, se regirá por lo dispuesto en el artículo 1939 del Código Civil.

En este sentido, el citado artículo 1939 del Código Civil, dispone que "La prescripción comenzada antes de la publicación de este código se regirá por las leyes anteriores al mismo; pero si desde que fuere puesto en observancia transcurriese todo el tiempo en él exigido para la prescripción, surtirá ésta su efecto, aunque por dichas leyes anteriores se requiriese mayor lapso de tiempo".

Lo anterior, sin perjuicio de la *obligación de conservación y custodia* de libros y documentos que incumbe al empresario, que se fija en *seis años* en el artículo 30 del Código de Comercio, de acuerdo con el cual:

> "1. Los empresarios conservarán los libros, correspondencia, documentación y justificantes concernientes a su negocio, debidamente ordenados, durante *seis años*, a partir del último asiento realizado en los libros, salvo lo que se establezca por disposiciones generales o especiales.
>
> 2. El cese del empresario en el ejercicio de sus actividades no le exime del deber a que se refiere el párrafo anterior y si hubiese fallecido recaerá sobre

sus herederos. En caso de disolución de sociedades, serán sus liquidadores los obligados a cumplir lo prevenido en dicho párrafo."

En *materia tributaria*, los artículos 66 al 70 de la Ley 58/2003, de 17 de diciembre, General Tributaria, fijan en *cuatro años* el plazo de *prescripción de las deudas tributarias*, sin perjuicio de lo dispuesto en sus artículos 115 y 148, referidos -respectivamente- a las potestades y funciones de comprobación e investigación, y al alcance de las actuaciones del procedimiento de inspección. Asimismo, de acuerdo con sus artículos 66 bis, 259.3 a) y 262, en ocasiones, podría resultar justificado el bloqueo de la información con datos de carácter personal por un plazo de *hasta diez* (10) años.

Por su parte, el artículo 131 del Código Penal -CP-, aprobado por Ley Orgánica 10/1995, de 23 de noviembre, establece el plazo de prescripción de los delitos, disponiendo que prescriben (…) *a los diez* (10) años aquellos cuya pena máxima señalada por la ley sea prisión o inhabilitación por más de cinco años y que no exceda de diez, y *a los cinco* (5) años los demás delitos, excepto los delitos leves y los delitos de injurias y calumnias, que prescriben al año.

En este sentido, tras las últimas modificaciones del Código Penal, operadas en virtud de la Ley Orgánica 7/2012, de 27 de diciembre, y de la Ley Orgánica 1/2019, de 20 de febrero, la regulación de los delitos contra la Hacienda Pública y contra la Seguridad Social -artículos 305 a 310 del CP-, contempla diversas posibilidades incardinadas en los distintos tipos penales contenidos en dichos preceptos, de los que deriva la imposición de penas de (i) prisión de uno a cinco años *-ex artículo 305.1-,* (ii) de prisión de tres meses a un año *-ex artículo 305.3-*, y (iii) de prisión de dos a seis años cuando el delito contra la Hacienda Pública se cometiere concurriendo alguna de las tres circunstancias tipificadas en el artículo 305 bis.

En consecuencia, con la introducción del nuevo tipo agravado del artículo 305 bis del CP para tipificar las conductas de cuantía superior a 600.000 euros -que se sancionan con una pena máxima de seis años-, y en aplicación del artículo 131 del propio CP, el plazo máximo de prescripción se fija en *diez (10) años.*

En materia de *seguridad social*, el artículo 21.1 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, se refiere a la obligación -que incumbe al empresario y a las entidades de formación- en orden a la conservación durante *cuatro años*, de la documentación o los registros o soportes informáticos en que se hayan transmitido los correspondientes datos que acrediten el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran

en relación con dichas materias, así como los documentos de cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones.

Dicho plazo se encuentra en consonancia con el fijado por el artículo 24 del Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, cuando dispone que:

> "1. Prescribirán a los *cuatro años* los siguientes derechos y acciones:
>
> a) El derecho de la Administración de la Seguridad Social para determinar las deudas por cuotas y por conceptos de recaudación conjunta mediante las oportunas liquidaciones.
>
> b) La acción para exigir el pago de las deudas por cuotas de la Seguridad Social y conceptos de recaudación conjunta.
>
> c) La acción para imponer sanciones por incumplimiento de las normas de Seguridad Social.
>
> 2. Respecto de las obligaciones con la Seguridad Social cuyo objeto sean recursos distintos a cuotas, el plazo de prescripción será el establecido en las normas que resulten aplicables en razón de la naturaleza jurídica de aquellas.
> (…)"

Por su parte, el artículo 4 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, se refiere a la prescripción de las infracciones en el orden social, disponiendo *con carácter general* -en su apartado 1- su prescripción en el plazo de *tres años*.

A su vez, según se establece en los apartados 2, 3 y 4 de dicho precepto, prescribirán (i) a los *cuatro años*, las infracciones cometidas en materia de Seguridad Social; (ii) al año, a los tres años o a los cinco años, dependiendo de su gravedad, las infracciones cometidas en materia de prevención de riesgos laborales, y (iii) a los tres meses, los seis meses, y al año -también en función de su gravedad-, las infracciones a la legislación de sociedades cooperativas. Dichos plazos han de computarse en todos los casos desde la fecha de la infracción.

También en relación con la Seguridad Social, se impone en este punto una referencia a los plazos de *prescripción de los delitos* establecidos en el artículo 131 del Código Penal, aprobado por Ley Orgánica 10/1995, de 23 de noviembre, cuando dispone que "prescriben (…) a los *diez (10) años* aquellos cuya pena máxima señalada por la ley sea prisión o inhabilitación por más de cinco años y que no exceda de diez, (…)" y "a los cinco (años), los demás delitos, excepto los delitos leves y los delitos de injurias y calumnias, que prescriben al año".

En este sentido, tras la reforma de operada por la Ley Orgánica 7/2012, de 27 de diciembre, los tipos penales agravados de los artículos 307 *bis* y 307 *ter* del CP fijaron en prisión de dos a seis años, la pena a imponer por la comisión de los injustos típicos de sus respectivos apartados 1 y 2.

En consecuencia, de acuerdo con la dicción literal de dichos preceptos, en consideración a la pena máxima prevista por estos tipos penales -de seis años-, y en aplicación del artículo 131 del propio CP, el plazo máximo de prescripción aplicable para estos supuestos es el de *diez (10) años.*

Finalmente, en lo relativo a prescripción de acciones en el *ámbito laboral*, debe recordarse que, según dispone el artículo 59 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, las acciones derivadas del contrato de trabajo que no tengan previsto plazo de prescripción específico están sometidas al plazo de *prescripción de un año*, de modo que:

> "1. Las acciones derivadas del contrato de trabajo que no tengan señalado plazo especial prescribirán *al año de su terminación*.
>
> A estos efectos, se considerará terminado el contrato:
>
> a) El día en que expire el tiempo de duración convenido o fijado por disposición legal o convenio colectivo.
>
> b) El día en que termine la prestación de servicios continuados, cuando se haya dado esta continuidad por virtud de prórroga expresa o tácita.
>
> 2. Si la acción se ejercita para exigir percepciones económicas o para el cumplimiento de obligaciones de tracto único, que no puedan tener lugar después de extinguido el contrato, el plazo de un año se computará desde el día en que la acción pudiera ejercitarse.
>
> 3. El ejercicio de la acción contra el despido o resolución de contratos temporales caducará a los veinte días siguientes de aquel en que se hubiera producido. Los días serán hábiles y el plazo de caducidad a todos los efectos.
>
> El plazo de caducidad quedará interrumpido por la presentación de la solicitud de conciliación ante el órgano público de mediación, arbitraje y conciliación competente.
>
> 4. Lo previsto en el apartado anterior será de aplicación a las acciones contra las decisiones empresariales en materia de movilidad geográfica y modificación sustancial de condiciones de trabajo. El plazo se computará desde el día siguiente a la fecha de notificación de la decisión empresarial, tras la finalización, en su caso, del periodo de consultas."

Tal y como se observa, la distinción de diferentes tipos de infracciones y plazos de prescripción traídos hasta aquí, encajan sustancialmente con las diversas categorías anunciadas por la entidad consultante en su consulta, mas -como se aprecia- no se compadece con las consecuencias obtenidas en orden a la determinación del plazo que en cada caso haya de justificar dicho bloqueo de la información personal de los trabajadores y antiguos trabajadores de la empresa.

V

Además de la documentación relativa a seguridad y salud laboral, control y registro de absentismo, y gestión del bonus por siniestralidad, la mercantil consultante se refiere a la necesidad de bloquear los *datos de salud* manejados por el servicio médico de empresa para, en su caso, dar respuesta a las posibles acciones que pudieren plantearse por los trabajadores afectados una vez finalizada la relación laboral. A este respecto, alude a las distintas acciones judiciales o requerimientos de información que, en materia laboral y administrativa, pudieren plantearse contra la empresa respecto de relaciones laborales ya extinguidas tanto por el propio extrabajador como por la autoridad laboral, así como a la actividad inspectora de la Inspección de Trabajo y Seguridad Social.

En el presente caso la consultante, en cuanto empleador, debe estar al estricto cumplimiento de la normativa sobre **"Prevención de Riesgos Laborales"** tanto durante la vigencia del contrato de trabajo cuanto -en su caso- una vez concluido este.

De tal modo, el establecimiento de plazos más amplios para la conservación de los datos de carácter personal de los trabajadores obrante en *determinados ficheros* de la consultante viene determinado directamente por la normativa aplicable, de acuerdo con los fines, requisitos y garantías establecidos en la misma.

A este respecto, el artículo 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, dispone que:

> "En los supuestos en que la naturaleza de los *riesgos inherentes* al trabajo lo haga necesario, el derecho de los trabajadores a la *vigilancia periódica* de su estado de salud deber ser prolongado *más allá de la finalización de la relación laboral*, en los términos que *reglamentariamente se determinen."*

La transcrita habilitación legal en orden al desarrollo reglamentario del plazo de obligatoriedad de la vigilancia periódica de la salud de los trabajadores se ha concretado en diversas normas jurídicas, algunas de las cuales elevan el plazo de conservación de determinados datos concernientes a la salud de los trabajadores, hasta los *cuarenta (40) años*.

Así, el artículo 9 del Real Decreto 664/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo, dispone:

"Artículo 9 Documentación

1. El empresario está obligado a disponer de:

a) La documentación sobre los resultados de la evaluación a que se refiere el artículo 4, así como los criterios y procedimientos de evaluación y los métodos de medición, análisis o ensayo utilizados.

b) Una lista de los trabajadores expuestos en la empresa a agentes biológicos de los grupos 3 y 4, indicando el tipo de trabajo efectuado y el agente biológico al que hayan estado expuestos, así como un registro de las correspondientes exposiciones, accidentes e incidentes.

2. El empresario deberá adoptar las medidas necesarias para la conservación de un registro de los historiales médicos individuales previstos en el apartado 5 del artículo 8 del presente Real Decreto, sin perjuicio de lo dispuesto en el artículo 22 de la Ley de Prevención de Riesgos Laborales.

3. La lista de los trabajadores expuestos y los historiales médicos **deberán conservarse durante un plazo mínimo de diez años después de finalizada la exposición; este plazo se ampliará hasta cuarenta años en caso de exposiciones que pudieran dar lugar a una infección en la que concurran alguna de las siguientes características**: (la negrita es nuestra)

a) Debida a agentes biológicos con capacidad conocida de provocar infecciones persistentes o latentes.

b) Que no sea diagnosticable con los conocimientos actuales, hasta la manifestación de la enfermedad muchos años después.

c) Cuyo período de incubación, previo a la manifestación de la enfermedad, sea especialmente prolongado.

d) Que dé lugar a una enfermedad con fases de recurrencia durante un tiempo prolongado, a pesar del tratamiento.

e) Que pueda tener secuelas importantes a largo plazo.

4. La documentación a que se refiere el párrafo b) del apartado 1 será adicional a la que el empresario deberá elaborar de acuerdo con el artículo 23 de la Ley de Prevención de Riesgos Laborales y estará sujeta al mismo régimen jurídico que ésta, en especial en lo que se refiere a su puesta a disposición de las autoridades laboral y sanitaria, y al acceso y confidencialidad de la información.

5. El tratamiento automatizado de datos personales sólo podrá realizarse en los términos previstos en la *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal."* *

*Nótese que, en el momento actual, este último apartado -5- ha de entenderse referido a la normativa vigente en materia de protección de datos.

En similares términos, el artículo 9 del Real Decreto 665/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo, establece que:

Artículo 9. Documentación.

1. El empresario está obligado a disponer de:

a) La documentación sobre los resultados de la evaluación a que se refiere el artículo 3, así como los criterios y procedimientos de evaluación y los métodos de medición, análisis o ensayo utilizados.

b) Una lista actualizada de los trabajadores encargados de realizar las actividades respecto a las cuales los resultados de las evaluaciones mencionadas en el artículo 3 revelen algún riesgo para la seguridad o la salud de los trabajadores, indicando la exposición a la cual hayan estado sometidos en la empresa.

2. El empresario deberá adoptar las medidas necesarias para la conservación de los historiales médicos individuales previstos en el apartado 3 del artículo 8 del presente Real Decreto, sin perjuicio de lo dispuesto en el artículo 22 de la Ley de Prevención de Riesgos Laborales.

3. Tanto la lista mencionada en el apartado 1 anterior como los historiales médicos mencionados en el apartado 2 **deberán conservarse durante cuarenta años después de terminada la exposición, remitiéndose a la autoridad laboral en caso de que la empresa cese en su actividad antes de dicho plazo.** (la negrita es nuestra)

Los historiales médicos serán remitidos por la autoridad laboral a la sanitaria, quien los conservará, garantizándose en todo caso la confidencialidad de la información en ellos contenida. En ningún caso la autoridad laboral conservará copia de los citados historiales.

4. El tratamiento automatizado de datos personales solo podrá realizarse en los términos previstos en la *Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal."* *

*Nótese que, en el momento actual, este último apartado -4- ha de entenderse referido a la normativa vigente en materia de protección de datos.

Por su parte, el artículo 18 del Real Decreto 396/2006, de 31 de marzo, por el que se establecen las disposiciones mínimas de seguridad y salud aplicables a los trabajos con riesgo de exposición al amianto, prevé también en este caso la conservación de los datos de exposición de los trabajadores y los datos referidos a la vigilancia sanitaria específica de los trabajadores por un plazo *mínimo de cuarenta (40) años* después de finalizada la exposición. En concreto, el apartado 4 de dicho artículo dispone que:

> "Artículo 18.4
>
> Los datos relativos a la evaluación y control ambiental, los datos de exposición de los trabajadores y los datos referidos a la vigilancia sanitaria específica de los trabajadores se conservarán durante **un mínimo de cuarenta años después de finalizada la exposición,** remitiéndose a la autoridad laboral en caso de que la empresa cese en su actividad antes de dicho plazo. (la negrita es nuestra)
>
> Los historiales médicos serán remitidos por la autoridad laboral a la sanitaria, quien los conservará, garantizándose en todo caso la confidencialidad de la información en ellos contenida. En ningún caso la autoridad laboral conservará copia de los citados historiales."

En otros casos, como el previsto el artículo 38 del Real Decreto 783/2001, de 6 de julio, por el que se aprueba el Reglamento sobre protección sanitaria contra radiaciones ionizantes, se fija en un *mínimo de treinta (30) años* el plazo de conservación de los datos de los afectados, debiendo archivarse y conservarse hasta que el *trabajador alcance la edad de setenta y cinco años, y nunca por un periodo inferior a treinta años, contados a partir de la fecha de cese* del trabajador en aquellas actividades que supusieran su clasificación como trabajador expuesto.

En consecuencia, en lo relativo a los trabajadores afectados por este tipo de tratamientos, los diferentes plazos a los que la consultante refiere la conservación de los datos personales resultarían conformes con lo dispuesto en la normativa de protección de datos, si bien únicamente en lo atinente al cumplimiento de sus obligaciones en materia de prevención de riesgos laborales, **y en relación con las finalidades previstas por la misma,** lo que excluye su posible conservación para cualquier otro fin.

En cualquier caso -como queda expuesto-, la conservación de estos datos de carácter personal deberá producirse únicamente en relación con los estrictamente necesarios para la finalidad pretendida -protección de la salud de los trabajadores - y en atención a lo dispuesto por la normativa de prevención de riesgos laborales, debiendo darse el debido cumplimento a lo dispuesto en el artículo 5 –"Principios relativos al tratamiento"- del RGPD.

Muy especialmente, a los efectos que aquí interesan, deberá estarse a lo dispuesto en las letras b), c) y f) del artículo 5.1, referidos a los **principios de limitación de la finalidad, minimización, e integridad y confidencialidad,** que resultan plenamente predicables en relación con la información que haya de incorporarse a ***uno o varios ficheros concretos*** destinados al pretendido fin.

> "5.1 Los datos personales serán:
> (…)
> b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; («**limitación de finalidad**»);
> c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («**minimización** de datos»);
> (…)
> f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («**integridad y confidencialidad**»)."

Además de los supuestos previamente analizados, otros casos a tener en cuenta en relación con la conservación de los datos personales de los afectados serían los propios previstos en la LOPDGDD. Así, el plazo de un mes en relación con los tratamientos de datos en materia de videovigilancia -al que se refiere su artículo 22-, o el de tres meses para las denuncias internas reguladas en su artículo 24, teniendo en cuenta que, en estos casos, así como en el de las operaciones del artículo 21, referido a los tratamientos relacionados con la realización de determinadas operaciones mercantiles, no procede el bloqueo de los datos personales, sino pura y simplemente su supresión física.

Por otra parte, el plazo al que se refiere el artículo 32.2 de la LOPDGDD resulta también predicable en relación con cualquier eventual *responsabilidad* relacionada con el propio *tratamiento de los datos personales*; en consecuencia, el plazo máximo del bloqueo para este supuesto será el de *tres años*, establecido en el artículo 78 de la LOPDGDD como plazo máximo de prescripción de *sus* infracciones.

A su vez, el artículo 82.1 RGPD, bajo el título "Derecho a indemnización y responsabilidad", dispone que "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos."

Dada la naturaleza jurídico-privada de la consultante, la acción reconocida en el artículo 82.1 tendrá naturaleza civil, pudiendo resultar del

perjuicio causado como consecuencia del hecho mismo del tratamiento. De este modo, con carácter general, el plazo de prescripción de dicha acción será el establecido en el Código Civil para la acción de responsabilidad extracontractual, siendo dicho plazo el de *un año*, previsto en el artículo 1968.2º del citado Código.

VI

Por lo demás, tal y como se expuso con anterioridad, en el marco del presente informe resulta imposible ofrecer una respuesta exhaustiva a todos y cada uno de los supuestos contenidos en la *"Guía de plazos máximos de conservación de datos personales"* de la consultante, quien, en relación con el bloqueo de datos personales deberá atender, de una parte, a los plazos de prescripción de las acciones que pudieran derivarse de las relaciones jurídicas de toda índole -mercantil, civil, social, etcétera- que la vinculan con las personas afectadas por el tratamiento de sus datos, y, de otra parte, a las normas sectoriales que resulten aplicables a su actividad.

En definitiva, corresponde al *responsable* del tratamiento -que es el que ha determinado su finalidad- decidir cuándo los datos han dejado de ser necesarios para la finalidad para la cual fueron recabados -decayendo la posibilidad de su tratamiento-, si bien, en algunas ocasiones, es el legislador quien fija un plazo de conservación determinado en relación con supuestos o materias concretas.

En consecuencia, resulta necesario que por la entidad consultante se proceda al *examen* pormenorizado de todos y cada uno de los tratamientos incorporados a su registro de "actividades de tratamiento", determinando para cada uno de los supuestos planteados, atendiendo al conjunto de circunstancias concurrentes (finalidad del tratamiento, tipos de datos tratados, sujetos afectados y su relación con la entidad, normativa aplicable, etc.) el plazo concreto durante el cual los datos deberán conservarse, adoptándose las garantías oportunas o, en su caso, mantenerse bloqueados como estadio previo a su destrucción y borrado físico.

En este sentido, las consecuencias sancionadoras derivadas del incumplimiento de sus obligaciones en materia de conservación de datos por parte del responsable del tratamiento se han puesto de manifiesto recientemente en el marco de diversos expedientes sancionadores incoados por la Agencia. Por todos, el procedimiento sancionador *PS/00076/2020*, en cuya virtud se impone a una entidad financiera una multa de 50.000 euros por conservar los datos personales del reclamante en sus ficheros con infracción de lo dispuesto en el artículo 5.1.b del RGPD.

En la citada resolución, se considera probado que la entidad reclamada conservaba en sus registros los datos personales del reclamante, pese a haber transcurrido 16 años desde su última relación comercial, ya que disponía de los

mismos cuando el reclamante acudió nuevamente a dicha entidad financiera para contratar un nuevo servicio financiero en septiembre de 2019. En consecuencia, se imputó a la entidad la comisión de la citada infracción del principio de limitación de la finalidad, de acuerdo con el cual los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines, así mismo se establece también la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento.

En este punto debe tenerse en cuenta, como novedad introducida por el RGPD, que la infracción del principio de limitación del plazo de conservación se tipifica en el artículo 83.5 a) del RGPD, que considera que la vulneración de los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9, se sancionarán con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

En este sentido, el artículo 72.1 de la LOPDGDD incluye entre las infracciones que se consideran muy graves y prescribirán a los tres años -en su *letra a*)- “El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679”, y, en su *letra n*), “El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible”.

En cuanto a la determinación del día inicial del cómputo para la prescripción, debe recordarse que, conforme a lo dispuesto en el artículo 1969 del Código Civil, “El tiempo para la prescripción de toda clase de acciones, cuando no haya disposición especial que otra cosa determine, se contará desde el día en que pudieron ejercitarse”, quedando el plazo interrumpido en los supuestos previstos en el propio Código.