

N/REF: 0048/2022

La consulta plantea si es conforme al 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 lo sucesivo) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo), el acceso por parte de las compañías de seguros de automóviles, en caso de siniestro y antes de una hipotética judicialización de los hechos, a la información que contienen el Registrador de Datos de Incidencias, previsto en el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019.

LDA (o la consultante) manifiesta que el acceso a la información que contiene el Registrador de Datos de Incidencias (EDR por sus siglas en inglés “Event Data Recorder”) podría servir a distintas finalidades que se derivan del régimen jurídico aplicable al sector asegurador, en concreto del Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor. (LRCSCVM en lo sucesivo), la Ley 50/1980, de 8 de octubre, de Contrato de Seguro, (LCS en lo sucesivo), o la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, (LOSSEAR en lo sucesivo), y a su reglamento de desarrollo aprobado por Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. (ROSSEAR), y que por tanto el uso de dicha información por las entidades aseguradoras podría encontrar legitimación en alguno de los supuestos que prevé el artículo 6 del RGPD.

I

Planteados los términos de la consulta, debe indicarse que para que un tratamiento de datos personales sea conforme al RGPD deben cumplirse, entre otros elementos del sistema de protección de datos, los principios de protección de datos contenidos en el artículo 5.1 del RGPD, a cuyo tenor los datos personales serán:

- a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

- b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
- c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
- 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 («exactitud»);
- e) 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»);
- 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»).

En efecto, deben cumplirse todos los principios de protección de datos, en el sentido de que la consulta se centra principalmente en qué base jurídica sería de aplicación al tratamiento propuesto, obviándose el análisis de adecuación a otros principios como el de limitación de finalidad.

Todo ello sin perjuicio de tener en cuenta otros aspectos relacionados con el derecho a la protección de datos que de modo directo o indirecto se vean afectados.

## II

La consulta se ha de resolver analizando en primer término la regulación específica de los Registradores de Datos de Incidencias (EDR por sus siglas en

inglés), que se concreta principalmente en el **Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019**, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinados a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes de los vehículos y de los usuarios vulnerables de la vía pública, (Reglamento 2019/2144 en lo sucesivo).

En el **artículo 3.13** se define como “registrador de datos de incidencias»: un sistema diseñado exclusivamente para registrar y almacenar parámetros e información críticos relacionados con una colisión, poco antes, en el transcurso e inmediatamente después de esta”

En el **artículo 6.4** se indica lo siguiente:

4. Los registradores de datos de incidencias cumplirán en particular los siguientes requisitos:

- a) los datos que puedan registrar y almacenar respecto del período poco antes, durante e inmediatamente después de una colisión incluirán la velocidad del vehículo, el frenado, la posición y la inclinación del vehículo en la carretera, el estado y la velocidad de activación de todos sus sistemas de seguridad, el sistema eCall basado en el número 112 integrado en los vehículos, la activación de los frenos y cualquier otro parámetro de entrada pertinente referido a los sistemas de seguridad activa a bordo y de prevención de accidentes; dichos datos tendrán un nivel elevado de precisión y garantía de perdurabilidad;
- b) no podrán desactivarse;
- c) el modo en que estos puedan registrar y almacenar datos será tal que:
  - i) funcionen en un sistema de bucle cerrado,
  - ii) **los datos recogidos por ellos se anonimicen y protejan frente a la manipulación y el uso indebido**, y
  - iii) los datos recogidos por ellos permitan identificar el tipo, la variante y la versión precisos del vehículo y, en particular, los sistemas activos de seguridad y de prevención de accidentes instalados en él, y
- d) los datos registrados por ellos **podrán ponerse a disposición de las autoridades nacionales, sobre la base del Derecho de la Unión o nacional, únicamente para la investigación y el análisis de accidentes**, en particular a efectos de la homologación de tipo de

sistemas y componentes y de comprobación del posible incumplimiento del Reglamento (UE) 2016/679, mediante una interfaz normalizada.

5. Un registrador de datos de incidencias **no podrá grabar y almacenar** los cuatro últimos dígitos de la sección del **indicador del vehículo correspondiente al número de identificación del vehículo ni ninguna otra información que pueda permitir identificar el vehículo concreto de que se trate, a su propietario o a su poseedor.**

Asimismo, también hay que traer a colación lo indicado en los Considerandos, 10, 13 y 14 del citado Reglamento:

(10) ...El progreso tecnológico de esos sistemas debe tenerse en cuenta en cada evaluación de la legislación vigente a fin de que esta tenga aplicabilidad en un futuro, y a la vez se atenga estrictamente a los principios de **respeto de la intimidad y de protección de datos, y a fin de reducir o eliminar accidentes y lesiones en el transporte por carretera.**

(13) La introducción de registradores de datos de incidencias que almacenen una serie de datos anonimizados cruciales del vehículo, junto con requisitos en materia de intervalo, precisión y resolución de datos, así como de su recogida, almacenamiento y recuperabilidad, a lo largo de un breve lapso de tiempo antes, durante e inmediatamente después de una colisión (por ejemplo, activados por el despliegue de un airbag) constituye un paso valioso para obtener datos más precisos y exhaustivos sobre accidentes. Por tanto, todos los vehículos de motor deben estar equipados con tales registradores. Esos registradores deben ser capaces de grabar y almacenar datos de manera que **los Estados miembros puedan utilizarlos para realizar análisis de seguridad vial y evaluar la eficacia de medidas concretas que se hayan adoptado, sin la posibilidad de identificar al propietario o al poseedor de un vehículo concreto sobre la base de los datos almacenados.**

(14) Todo tratamiento de datos personales, como la información sobre el conductor tratada en los registradores de datos de incidencias o la información relativa a la somnolencia y la atención, o la distracción del conductor, **debe efectuarse de conformidad el Derecho de la Unión en materia de protección de datos, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (6).** Los registradores de datos de incidencias deben funcionar en un sistema de bucle cerrado en el que los datos almacenados se reescriban y **que no**

**permita identificar al vehículo ni al titular de los datos.** Además, los sistemas de advertencia de somnolencia y de pérdida de atención del conductor o los sistemas avanzados de advertencia de distracciones del conductor no deben registrar ni conservar de manera continuada ningún dato que no sea necesario para los fines para los que los datos fueron recogidos, o tratados de otro modo, dentro del sistema de bucle cerrado.

De la lectura de los preceptos y considerandos transcritos se extraen las siguientes conclusiones:

En primer lugar, que la finalidad “única” recogida en la norma (Derecho de la Unión) a la que sirve la recogida de datos de los EDR es para que las autoridades de los Estados Miembros con competencias en materia de tráfico analicen la seguridad vial y evalúen la eficacia de las medidas concretas que se hayan adaptado en ese aspecto, a partir de los datos obtenidos en la investigación y análisis de accidentes.

Es decir, **los destinatarios de la información son las autoridades con competencia en materia de tráfico y seguridad vial de los Estados Miembros y tiene como fin último la mejora en la elaboración de las políticas públicas de seguridad vial.**

En segundo lugar, que la información que se obtiene por los EDR debe estar dotada de garantías de privacidad, en el sentido de que **no puede identificarse ni el vehículo, ni el propietario ni el poseedor del mismo, en definitiva, que no pueda atribuirse la información obtenida del EDR al titular de los datos, evitando así la identificación y en último término, la individualización o singularización.**

Y en tercer y último lugar, se hace una remisión al cumplimiento del RGPD respecto del tratamiento de los datos obtenidos por el EDR, de lo que se infiere sin ningún género de dudas, que **se exige el cumplimiento, entre otras cuestiones, de los principios de protección de datos.**

### III

En segundo término, desde la perspectiva del derecho a la protección de datos, el tratamiento objeto de análisis que se deriva del citado Reglamento 2019/2144 consistente en el uso de la información que consta en el EDR, debe tenerse en cuenta que se realiza al amparo de los apartados c) y e) del artículo 6.1 del RGPD a cuyo tenor:

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

Por su parte, el apartado 3 del citado artículo 6 del RGPD nos indica que:

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: **a) el Derecho de la Unión**, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. **La finalidad del tratamiento deberá quedar determinada en dicha base jurídica** o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: **las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo**, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

En el presente caso, ha sido el Derecho de la Unión el que ha previsto la injerencia en el derecho a la protección de datos que supone el acceso al EDR, a la vez que ha determinado la necesidad de que dicha injerencia se realice con ciertos límites que operan como garantías y que se concretan en las medidas tendentes a evitar o impedir la identificación directa, o indirecta del vehículo, del titular o incluso de su poseedor.(estas desaparecerían en el tratamiento que propone la consultante pues se asociarían al conductor del vehículo y en su caso, al tomador del seguro).

Se trata, de una restricción al derecho fundamental a la protección de datos justificada por el hecho de proteger otro bien jurídico como es la seguridad del tráfico de vehículos, la prevención de accidentes y en última instancia la elaboración de políticas públicas en la materia con la máxima eficacia.

**En definitiva, es la propia norma, el Derecho de la Unión, el que legitima el uso del EDR y el que define claramente la finalidad, los destinatarios de dicha información y las garantías que se han de observar.**

#### IV

Llegados a este punto debe traerse a colación el criterio de esta Agencia sobre las exigencias legales referidas a las limitaciones del derecho fundamental a la protección de datos.

El Informe 89/2020 aborda, entre otras cuestiones, el uso posterior de datos personales derivado de un tratamiento que se realiza en cumplimiento de una obligación legal (publicación en boletines oficiales), y recuerda los requisitos que han de darse para la limitación de este derecho fundamental:

(...)

Por ello, tal y como se ha ido adelantando, cuando se trata de la publicación de datos personales al amparo de las previsiones contenidas en las letras c) o e) del RGPD, debe tenerse en cuenta la jurisprudencia y la doctrina de esta Agencia respecto a los requisitos para legitimar la misma, al objeto de respetar el principio de proporcionalidad y establecer las garantías oportunas.

En este sentido, esta Agencia viene reiterando cómo, en los supuestos del artículo 6.1., letras c) y e), el RGPD contiene previsiones específicas al respecto, comenzando con las previstas en su propio artículo 6, apartados 2 y 3, cuya redacción es la siguiente:

(...)

Por otro lado, debe tenerse igualmente en cuenta que, en el caso de que la obligación venga impuesta por una norma de derecho interno, la misma deberá tener rango de ley, por exigirlo el artículo 53.1 de la Constitución, tal y como expresamente recoge el artículo 8.1 de la LOPDGDD, añadiendo que “podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679” y deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente, en las sentencias 292/2000 de 30 noviembre y 76/2019 de 22 de mayo, conforme a la cual los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el



legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, siendo la propia ley la que habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El Tribunal Constitucional (TC) ha sido claro en cuanto a que la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata, en definitiva, de “garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”. Tampoco sirve por ello que para el establecimiento de dichas garantías adecuadas y específicas la ley se remita al propio RGPD o a la LOPDGDD.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o



equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [ RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [ RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [ RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [ RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [ RTC 2000, 186] , F. 6).”

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

Pues bien, la STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos

fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos.

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].

La ya citada STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las categorías especiales de datos:

68 (...) Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15

(Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

En consecuencia, los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.

(...)

La propuesta de la consultante, pretendiendo basar el acceso al EDR en las normas que cita, resulta contraria a lo que se acaba de indicar, por cuanto pretende dar una finalidad distinta a la información que se obtiene del EDR, con actores distintos y sin observar las garantías previstas.

Sobre todo, **teniendo en cuenta que estos elementos son perfectamente delimitados en el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019, que es a su vez, la base de legitimación del tratamiento.**

#### IV

Teniendo en cuenta lo anterior debe concluirse que **el tratamiento que propone la consultante no cumple con el principio de licitud.**

**En efecto, el tratamiento de la información que consta en el EDR, previsto en el Reglamento 2019/2144 se realiza en cumplimiento de una obligación legal y para cumplir una misión de interés público, es decir, al margen de la voluntad del interesado y con expresas garantías para salvaguardar su privacidad. Esta circunstancia requiere que la injerencia propuesta por la consultante esté prevista en el Derecho de la Unión o en el derecho nacional a través de normas que cumplan los requisitos que se han ido poniendo de manifiesto.**

Así, cabe exponer que el RGPD tiene por objeto, como recuerda el TJUE, proporcionar un elevado nivel de protección del derecho fundamental de protección de datos personales. Sentencia del TJUE de 28 de abril de 2022, C-319/20, Meta Platforms Ireland, apartado 73 (entre otras muchas):

*73 Tal interpretación es conforme con las exigencias derivadas del artículo 16 TFUE y del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y, por lo tanto, con el **objetivo***

***perseguido por el Reglamento General de Protección de Datos de garantizar una protección eficaz de las libertades y de los derechos fundamentales de las personas físicas y, en particular, de garantizar un elevado nivel de protección del derecho de toda persona a la protección de los datos de carácter personal que le conciernan (véase, en este sentido, la sentencia de 15 de junio de 2021, Facebook Ireland y otros, C-645/19, EU:C:2021:483, apartados 44, 45 y 91).***

De ello se desprende que cuando la norma de Derecho de la Unión o del Estado Miembro establece que unos determinados tratamientos de datos, que la norma en cuestión establece con carácter obligatorio, tienen una determinada finalidad, excluyendo otras, (como se demuestra por el uso de la expresión que utiliza la norma “los datos registrados por ellos podrán ponerse a disposición de las autoridades nacionales, sobre la base del Derecho de la Unión o nacional, **únicamente** para la investigación y el análisis de accidentes”), y para lo cual el legislador establece determinadas cautelas y garantías específicas, no es posible un tratamiento para una finalidad diferente de la prevista por la norma sobre una base jurídica diferente de la propia norma que ha establecido dicho tratamiento, por cuanto dicha finalidad sería, por expresa decisión del legislador “incompatible” con cualquier finalidad que no sea la expresada en la norma que establece el tratamiento (de ahí la expresión “únicamente”). Ello es, por otra parte, consistente con el objetivo ya expuesto del RGPD de garantizar una protección eficaz de las libertades y de los derechos fundamentales de las personas físicas y, en particular, de garantizar un elevado nivel de protección del derecho de toda persona a la protección de los datos de carácter personal. Por eso, no sería conforme con el propio RGPD tratar de utilizar esta norma para unos tratamientos expresamente excluidos por el propio legislador que ha impuesto el tratamiento para unos fines concretos, excluyendo cualquier otro.

En consecuencia, no se cumpliría el principio de licitud previsto en el artículo 5.1 a) del RGPD para el tratamiento previsto en la consulta, ni tampoco el de limitación de la finalidad del art. 5.1.b) RGPD, por cuanto el legislador ha establecido que la finalidad del tratamiento es “únicamente” la prevista en el Reglamento 2019/2144, por lo que la finalidad solicitada en el informe no se considera compatible por haberlo excluido expresamente el legislador. No estamos ante tratamientos ulteriores con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, por lo que el tratamiento no sería posible y resulta ya innecesario el análisis de otros principios pues el tratamiento no podría llevarse a cabo.