La consulta plantea una serie de cuestiones que conviene analizar por separado, si bien todas tienen como hilo conductor el ejercicio de las competencias de la entidad consultante.

I

En la primera de las cuestiones planteadas se hace referencia a la elaboración de las fichas con los datos tanto de víctimas mortales como de víctimas no mortales en actuaciones de violencia de género. Se expone cuál es el contenido y "recorrido" (iter) de los datos personales que se recogen en dichas fichas. La pregunta que se hace es si dicho contenido y su recorrido cumple con los principios de la LOPD, y de modo especial con los estándares de seguridad establecidos para los datos relativos a violencia de género (medidas de seguridad de nivel alto).

Empezando por este último aspecto cabe decir que se ha producido una modificación sustancial entre lo preceptuado (i) en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD), y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, (RLOPD) y (ii) el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD). En esta última norma, aplicable plenamente a partir del 25 de mayo de 2018, no se establece un elenco de medidas de seguridad específicas que el responsable del tratamiento habrá de establecer en todo caso, como se hacía en la LOPD y RLOPD, sino que en virtud del principio de responsabilidad activa, el art. 32 RGPD establece:

> *Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Por tanto, corresponde al responsable del tratamiento, con la ayuda, en su caso, del Delegado de Protección de Datos (DPD), la determinación de las concretas medidas necesarias para la seguridad y confidencialidad de los datos manejados.

En relación con dichas medidas de seguridad, teniendo en cuenta el recorrido de los datos tal y como ha sido expuesto en la consulta, desde el momento en que se tratan datos particularmente sensibles (situación de discapacidad, en su caso; identificación de víctima y agresor etc.), parece que las fichas se remiten por correo electrónico a una dirección corporativa gestionada por una determinada subdirección; nada se dice de las medidas técnicas u organizativas aplicadas a dicho correo electrónico para evitar su apertura, lectura o utilización por quien no tenga necesidad de acceso a dichos datos. Tampoco de las medidas técnicas y organizativas aplicadas al tratamiento que se realiza en la Subdirección General de sensibilización, prevención y conocimiento para evitar igualmente su acceso por personas entre cuyas funciones no se incluyen el tratamiento de dichos datos.

En cuanto al contenido de las fichas, y dado que se inquiere respecto de los principios aplicables en la normativa protección de datos personales, hay que decir que en este caso el aplicable es el principio de “minimización de datos”. De conformidad con el artículo 5.1 c) del RGPD, los datos personales serán c) *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»).* Cuáles han de ser exactamente los datos incluidos en dichas fichas desde el punto de vista del principio de minimización de datos, corresponde decidirlo al responsable del tratamiento, quien habrá de realizar un examen del contenido de las fichas, ahora que parece que se van a modificar en su formato, para no incluir en ellas ningún dato que sea superfluo o innecesario a las actividades, finalidades y propósitos para los que sirve en dichas fichas. En ese caso, el tratamiento de datos personales que no sea necesario en relación para los fines para los que van a ser tratados se consideraría contrario a la normativa de protección de datos personales.

En cuanto al recorrido de los datos, resulta difícil pronunciarse sobre si puede haber un recorrido inferior que minimice los riesgos asociados al tratamiento de datos personales de categorías sensibles en una cadena de múltiples eslabones. En principio, a la vista de la exposición en la consulta, parece adecuado, sin perjuicio de mencionar que en el caso de que se

pudieran reducir los escalones a seguir en el envío de los datos personales ello produciría una disminución del riesgo de dispersión de los mismos y por tanto se reduciría el riesgo de una infracción a la normativa en materia de datos personales, por lo que corresponderá igualmente al responsable del tratamiento *la aplicación de las medidas organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo* (art. 32.1 RGPD).

II

Sobre el secreto estadístico, es obvio que la normativa relativa al secreto estadístico se aplica cuando nos encontramos ante datos estadísticos. Así, el art. 13 de la ley 12/1989, de 9 de mayo, de la Función Estadística Pública establece:

> *Artículo 13.*
>
> *1. Serán objeto de protección y quedarán amparados por el secreto estadístico los datos personales que obtengan los servicios estadísticos tanto directamente de los informantes como a través de fuentes administrativas.*
>
> *2. Se entiende que son datos personales los referentes a personas físicas o jurídicas que o bien permitan la identificación inmediata de los interesados, o bien conduzcan por su estructura, contenido o grado de desagregación a la identificación indirecta de los mismos.*
>
> *3. El secreto estadístico obliga a los servicios estadísticos a no difundir en ningún caso los datos personales cualquiera que sea su origen.*

Por lo tanto, la normativa estadística protege también los datos que tenga la consideración de “estadísticos” aunque se trata de personas fallecidas, o sean relativos a personas jurídicas.

Ahora bien, ello se aplica con carácter general a todo dato que tenga carácter de “estadístico”; pero el art. 14 establece la posible excepción de comunicación de los datos y remite al art. 15. En su apartado 1 dicho artículo 15 hace referencia a la comunicación a efectos estadísticos, y en su apartado 2 hace referencia a la comunicación a efectos “no estadísticos” de la información que obra en los registros públicos, la cual no estará sujeta al secreto estadístico sino a la legislación específica que en cada caso será de aplicación. Por ello, para la comunicación a efectos “no estadísticos” se estará sujeto a lo establecido en la normativa que en cada caso sea de aplicación, y a su vez dicho tratamiento de datos estará, por supuesto, sujeto a la normativa de protección de datos personales cuando ésta sea aplicable.

En un supuesto en el que se planteaba si se divulgaban o no los datos personales de víctimas o heridos en un accidente aéreo, esta AEPD en Informe de fecha 12 de noviembre de 2008 emitido en respuesta a consulta formulada por el Director General de Aviación Civil, que en esencial, su doctrina sería de aplicación al caso expuesto, expone:

"XII

De lo que se ha venido indicando hasta el presente lugar cabe extraer varias conclusiones que permitirían considerar amparado en la Ley Orgánica 15/1999 la divulgación de los datos de los pasajeros y tripulantes de la aeronave.

Así, por una parte, ya se ha indicado que la citada comunicación podría resultar necesaria para salvaguardar un interés vital de los pasajeros y tripulantes, dado que a través de la misma podrá procederse a su identificación, tanto si han fallecido como si se encontrasen impedidos para llevarla a cabo por sí mismos.

Además, la publicación de la lista permitiría facilitar a la compañía y a los servicios que se encontrasen atendiendo la situación de emergencia causada por el siniestro datos relacionados con la salud de los pasajeros y tripulantes que puedan resultar imprescindibles para llevar a cabo una adecuada asistencia sanitaria de aquéllos, tales como la existencia de determinadas enfermedades, inmunodeficiencias o alergias padecidas por aquellos. Dicha información pudiera ser facilitada, en su caso, por profesionales que no se encontrarían directamente vinculados con los pasajeros o tripulantes por una relación afectiva o familiar, sino que conociesen de esa información como consecuencia del previo tratamiento médico realizado a aquéllos.

Asimismo, la existencia de un siniestro en el que se produjese un elevado número de víctimas mortales y heridos exige la localización de las personas vinculadas a las mismas por razones familiares o afectivas análogas. Dichas personas no son conocidas a priori por la compañía aérea, al no ser exigible ese conocimiento por parte de la misma, ni siquiera en el supuesto de los miembros de la tripulación, siendo preciso dar a conocer públicamente la información mínima sobre los pasajeros o tripulantes que permita esa rápida localización.

Del mismo modo, y como contrapartida de lo anterior, la producción del siniestro general un derecho en las personas vinculadas con las víctimas o potenciales víctimas de conocer si sus allegados se encuentran entre los que han sufrido el siniestro. Ese derecho, en cierto modo vinculado con el derecho fundamental a recibir información veraz, debe

equilibrarse con el derecho fundamental a la protección de datos de las víctimas del accidente, prevaleciendo sobre aquél siempre que la información difundida se refiera a los datos identificativos de las víctimas, suficientes para conocer si la persona allegada se encontraba o no a bordo de la aeronave.

Por último, la identificación de posibles beneficiarios de las indemnizaciones que hayan de ser satisfechas por la compañía aérea en cumplimiento de las normas vigentes en materia de responsabilidad en caso de fallecimiento o concurrencia de lesiones o daños personales en el pasaje exige que la misma adopte las medidas necesarias para que quienes ostentes esa condición tengan conocimiento "sin demora" de la misma.

XIII

La conclusiones alcanzadas en el apartado anterior de este informe permiten concluir que la divulgación por la compañía aérea de los datos meramente identificativos del pasaje y tripulación a bordo de una aeronave siniestrada se encontraría amparada por los artículos 11.2 c) y 11.2 e) de la Ley Orgánica 15/1999, en conexión con las letras b), d) y f) del artículo 7 de la Directiva 95/46/CE, no suponiendo dicha publicación vulneración alguna de la normativa reguladora del derecho fundamental a la protección de datos de carácter personal."

Por ello, en definitiva, y en respuesta a la concreta pregunta planteada, la comunicación a efectos no estadísticos estará sujeto la legislación específica que en cada caso será de aplicación, debiendo tenerse en cuenta, además, en su caso, la normativa de protección de datos personales.

III

A continuación, la consultante expone que las labores de seguimiento en los casos de violencia de género implican en muchos casos la necesidad de compartir información entre profesionales de distintos ámbitos y administraciones, y cita la ley 27/2003, reguladora de la orden de protección, que específicamente incluyó un art. 544 ter en la ley de enjuiciamiento criminal (LECr.) cuyo apartado 8, -continúa- establece que en caso de adoptarse dicha orden de protección por el Juez, las Administraciones públicas habrán de adoptar medidas de protección, sean éstas de seguridad o de asistencia social, jurídica, sanitaria, psicológica o de cualquier otra índole. A estos efectos se establecerá reglamentariamente un sistema integrado de coordinación administrativa que garantice la agilidad de estas comunicaciones.

Además de dicho apartado 8 es conveniente resaltar lo establecido en el apartado 5 de dicho artículo 544 Ter de la LECr, según el cual, 5. *la orden de protección confiere a la víctima de los hechos mencionados en el apartado 1 un estatuto integral de protección que comprenderá las medidas cautelares de orden civil y penal contempladas en este artículo y aquellas otras medidas de asistencia y protección social establecidas en el ordenamiento jurídico. La orden de protección podrá hacerse valer ante cualquier autoridad y Administración pública.*

El legislador ha pretendido por tanto establecer con dicha expresión de "estatuto integral" que a las víctimas de violencia de género habrán de aportárseles aquellas medidas de protección y asistencia social que requiera su situación.

Por ello, aún el caso de que los datos personales que puedan tratarse estos efectos contuvieran datos incluidos en las categorías especiales de datos personales a que hace referencia al artículo 9 RGPD, la prohibición que contiene el apartado 1 del mismo no sería aplicable cuando concurra la excepción establecida en la letra g) del apartado 2 de dicho artículo 9, según el cual: *el tratamiento es necesario por razones de un* ***interés público esencial****, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;*

En el presente caso, el tratamiento de los datos personales necesarios para la protección integral de las víctimas de violencia de género cabe considerarlo un interés público esencial, y es además proporcional al objetivo perseguido.

Por ello, y en respuesta a la concreta pregunta planteada, cabe decir que esta Agencia considera suficiente la previsión legal contenida en las modificaciones introducidas en la ley de enjuiciamiento criminal por la ley 27/2003 para posibilitar el intercambio de información entre los profesionales dedicados a la asistencia social, sanitaria, psicológica o de otra índole a las víctimas de violencia de género.

Lo anterior se entiende, por supuesto, siempre que concurran los requisitos para el tratamiento de dichos datos personales previstos en el artículo 5 y 6; es decir, siempre que en el tratamiento de los datos personales se cumplan los principios establecidos en el artículo 5 (el tratamiento de los datos personales habrá de realizarse para el cumplimiento de la finalidad -protección a las víctimas de violencia de género- para los que fueron obtenidos; los datos han de ser exactos; se garantice la integridad y confidencialidad de los datos etc.) Y en cuanto a la licitud del tratamiento, prevista en el art. 6, deberá concurrir al menos una de las causas de licitud que permiten el

tratamiento de dichos datos, entre las que cabe destacar que dicho tratamiento de datos sería necesario para cumplimiento de las obligaciones legales aplicables al responsable del tratamiento, o bien podría considerarse dicho tratamiento necesario para proteger intereses vitales del afectado.

IV

A continuación, la consulta inquiere sobre determinadas solicitudes de datos realizadas al centro de control del sistema (COMETA) por las Fuerzas y Cuerpos de Seguridad del Estado. Se refiere a consultas que las fuerzas de seguridad realizan en relación con los datos personales que constan el sistema de seguimiento por medios telemáticos en el ámbito de violencia de género; es decir, datos de usuarios (víctimas, o inculpados) del sistema de seguimiento telemático (pulseras con GPS y sistema de aviso si se entra en un radio de seguridad en torno a la víctima). Se aportan ejemplos de estas peticiones.

Los tratamientos de datos por las fuerzas y cuerpos de seguridad para la investigación y prevención de delitos se rigen por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (Directiva 2016/80). Dicha directiva aún no ha sido transpuesta al derecho español, por lo que la disposición transitoria cuarta del proyecto de ley orgánica de protección de datos actualmente en tramitación parlamentaria en las Cortes establece que dichos tratamientos continuarán rigiéndose por la LOPD, y en particular por su artículo 22, y por sus disposiciones de desarrollo, en tanto no entre en vigor la norma que transponga al derecho español lo dispuesto en la citada directiva.

En consecuencia, a los tratamientos de datos realizados por las fuerzas y cuerpos de seguridad le sería aplicable el art. 22 LOPD, y por lo tanto también seguiría siendo aplicable la doctrina sentada por esta Agencia en los tan reiterados informes (entre otros) 0133/2008 y 0297/2005, que, en esencia, dicen así:

> *[…] deberán distinguirse aquellas actuaciones de la Policía Judicial que son llevadas a cabo en cumplimiento de un mandato judicial o de un requerimiento efectuado por el Ministerio Fiscal de aquéllas otras que se llevan a cabo por propia iniciativa o a instancia de su superior jerárquico.*
>
> *Respecto de las primeras resulta aplicable el artículo 11.2 d) de la Ley Orgánica 15/1999, no requiriéndose el consentimiento del interesado a la*

cesión, por cuanto los efectivos de la Policía Judicial solicitantes de los datos no son sino meros transmisores de la solicitud efectuada por el Ministerio Fiscal o el Órgano Jurisdiccional, actuando éste en el cumplimiento de las funciones que le han sido legalmente atribuidas y siendo el propio Juzgado o Tribunal o el Ministerio Fiscal el destinatario de los datos cedidos, como exige el artículo referido.

El problema se plantea, sin embargo, en relación con aquellos supuestos en los que la Policía Judicial requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del responsable, al no existir en ese caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión.

En este caso nos encontramos, a nuestro juicio, ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Resultará, en consecuencia, aplicable a este segundo supuesto lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999, según el cual "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad"

El citado artículo habilita, a nuestro juicio, a los miembros de la Policía Judicial para la obtención y tratamiento de los datos requeridos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando, como se indica en el informe de la Comisaría General de la Policía Judicial adjunto a la consulta y esta Agencia Española de Protección de Datos ha venido indicando reiteradamente, se cumplan las siguientes condiciones:

a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.

b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.

c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.

d) Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

Con referencia a la última de las conclusiones señaladas, debe indicarse que, tratándose de actuaciones llevadas a cabo en el ámbito de las competencias consagradas en el apartado a) del artículo 445.1 de la Ley Orgánica del Poder Judicial, encontrándose por ello la Policía Judicial obligada a dar cuenta de los hechos a la Autoridad Judicial y Fiscal de forma inmediata, deberá procederse a la destrucción del registro de los datos obtenidos, una vez producida esa comunicación.

A mayor abundamiento, debe recordarse que, conforme dispone el artículo 11.2 d) de la Ley Orgánica 15/1999, procederá la cesión si ésta tiene por destinatario al Ministerio Fiscal o los Jueces o Tribunales, lo que, conforme se ha señalado, ocurre en el presente supuesto, dada la obligación de los miembros de la Policía Judicial de poner los datos que hayan sido obtenidos en conocimiento de la Autoridad Judicial o Fiscal. Por ello, la cesión solicitada tendrá amparo no sólo en el artículo 22.2 de la Ley Orgánica 15/1999, sino también en el propio artículo 11.2 d) de la misma.

Sobre la base de la doctrina contenida en estos informes cabe entonces responder a las preguntas realizadas en la consulta.

A la primera, es que, efectivamente, deberán ser atendidas las solicitudes por el centro de control cuando procedan de las unidades de policía judicial de las fuerzas y cuerpos de seguridad, de acuerdo con los fundamentos expuestos, y si se cumplen las condiciones exigidas. Ello supone, por otra parte, que sea de plasmar, siquiera sea mínimamente de forma que no pueda poner en peligro la investigación pero de manera que el responsable del tratamiento pueda tener la certeza de que la solicitud de información planteada cumple con los requisitos expuestos, esto es, que pueda determinar (por cuanto sigue siendo responsable del tratamiento, y de la cesión de datos que supone el dar la información a la policía desde el punto de vista la normativa de protección de datos) si la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación

concreta; que sea una petición concreta y específica, no genérica o meramente difusa; que la petición está expresamente motivada en relación con las circunstancias anteriores; y que posteriormente los datos obtenidos por la policía judicial serán cancelados cuando no fueran necesarios para la averiguación que motivó su petición.

Este régimen específico se aplica exclusivamente a las fuerzas y cuerpos de seguridad que actúen en el ámbito de los requisitos o características señalados, fundamentalmente cuando su actuación tenga por objeto bien la prevención de un peligro real para seguridad pública o la represión de infracciones penales; no en caso distinto, en cuyo caso el artículo 22.1 LOPD establece que los datos que se recojan para fines administrativos por las fuerzas y cuerpos de seguridad estarán sujetos al régimen general previsto en dicha ley.

La tercera pregunta queda contestada con lo respondido en la primera de estas: efectivamente, deberán acreditar suficientemente, en el ámbito de los requisitos mencionados, las condiciones y la finalidad de su solicitud justificándolo con arreglo a las características ya reiteradas.

En cuanto a si es necesario que se formalicen por escrito las peticiones de las fuerzas y cuerpos de seguridad, hay que decir que el RGPD establece que es responsabilidad del responsable del tratamiento el demostrar las características y condiciones del mismo. Así, el art. 24.1 RGPD dice:

> *Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de* ***garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento****. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

En consecuencia, corresponde al responsable determinar si es necesario una petición por escrito o, atendiendo a las circunstancias, será suficiente efectuarse por teléfono. Desde un punto de vista de prudencia valorativa, cabe decir que se considera mejor en todo caso una petición escrita en la que consten por escrito de manera detallada las circunstancia requeridas en los informes citados para determinar si el tratamiento/cesión de datos personales a las fuerzas de seguridad cumple con los requisitos mencionados. Ciertamente, en determinados casos de urgencia ante un peligro real o la prevención de una infracción penal podrían darse casos en que se solicitan los datos telefónicamente, pero habrían de ser forzosamente excepciones a la regla general. En cualquier caso, y aunque se realizasen por teléfono de manera excepcional, ello no es óbice para que también se requieran forzosamente que se expongan las razones que determinan que el tratamiento

de datos solicitado pueda ser considerado lícito; esto es, aunque se realice por teléfono deberán exponerse las circunstancias de que se solicita para la prevención de un peligro grave real o para el seguimiento de una infracción penal, ser suficientemente detallada, su motivación respecto a los dos anteriores etc. En cuanto a la forma en que una conversación telefónica puede acreditarse, la propia entidad consultante reconoce que se graban las conversaciones con los usuarios del sistema telemático de control, y que las peticiones de datos que se realizan son precisamente del centro de control de dicho sistema telemático, por lo que la respuesta habrá de ser que dichas conversaciones con las fuerzas y cuerpos de seguridad deberían de ser grabadas, con la advertencia expresa al interlocutor de dicha circunstancia, y posteriormente, en su caso, documentarse, para que el responsable del tratamiento pueda tener constancia en caso de que le fuera requerido información acerca de la cesión de datos que se ha realizado y la motivación y fundamentación aducida por el solicitante para ello.

En cuanto a la solicitud de comunicación de otros datos de los usuarios del sistema como el número de teléfono del dispositivo de localización o el número de teléfono particular de los usuarios, hay que proseguir con el razonamiento anterior, que cabe resumir diciendo que si dichos datos los tiene un órgano administrativo (pues la UTE que realiza físicamente dichas tareas es un encargado del tratamiento) con mayor razón podrán solicitarlo y obtenerlo las fuerzas y cuerpos de seguridad que se encargan de la investigación de infracciones penales o la prevención de riesgos graves para la seguridad pública. Pero ello siempre en el bien entendido de que dichos datos, para solicitarlos, se han de razonar y motivar de la misma manera y con las cuatro características y requisitos que hemos plasmado anteriormente, de manera que ha de ser siempre motivado, detallada en relación con una petición concreta, justificando que se realiza la petición para la prevención de un riesgo para la seguridad pública o la investigación de una infracción penal etc.

V

En cuanto a las cuestiones en relación con el derecho de acceso de los usuarios a los datos personales existentes en el sistema de control telemático, en relación con la normativa de protección de datos, esta Agencia considera, a tenor de la exposición que realiza la consulta, que la actuación del consultante al respecto ha sido correcta en las tres cuestiones planteadas.

El RGPD regula el derecho de acceso del interesado en su artículo 15, especificando su apartado 3 que el responsable del tratamiento facilitará una copia de los datos personales objeto del tratamiento, pero su apartado 4 se encarga de establecer que el derecho a obtener copia mencionado en el

apartado anterior no afectará negativamente a los derechos y libertades de otros.