



**CN10-029**

**DICTAMEN QUE SE EMITE EN RELACION CON LA CONSULTA FORMULADA POR XXXXX DE OSAKIDETZA-SERVICIO VASCO DE SALUD EN RELACIÓN A DIFERENTES DUDAS QUE LE SURGEN SOBRE CESIÓN O COMUNICACIÓN DE DATOS DE CARÁCTER PERSONAL A LAS FUERZAS Y CUERPOS DE SEGURIDAD.**

## **ANTECEDENTES**

**PRIMERO.** Con fecha 22 de noviembre de 2010 tuvo entrada en la Agencia Vasca de Protección de Datos solicitud de informe remitido por XXXXX de Osakidetza-Servicio Vasco de Salud en el que se señala lo siguiente:

*“...miembros de los Cuerpos y Fuerzas de Seguridad del Estado, han requerido al personal de un Centro de Salud que ofrezcan datos personales, tales como dirección, teléfono de contacto, etc., (sin haber requerido datos sobre diagnóstico o contenido del Historial Clínico) para fines policiales de investigación.*

*En primer lugar, debemos indicar que la investigación policial no ha sido formulada por escrito ni motivada de forma concreta y específica, ni consta que se produzca bajo requerimiento judicial, o del Ministerio Fiscal.*

*Se han solicitado datos personales no sanitarios, si bien nos surge la duda sobre otras actuaciones en el supuesto de requerir datos sobre citas, consultas, historial clínico, etc.*

*...Esta Dirección es consciente que los datos relativos a la salud de los ciudadanos son especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión. El objetivo de la presente consulta es el respeto a la intimidad y confidencialidad de datos personales como obligación inherente a la labor de la administración sanitaria.*

*Consideramos que las excepciones a dicha protección especial se debe de dar de forma motivada ante el riesgo grave para la salud de la colectividad, o prevención de un peligro real para la seguridad pública, o la represión de*



*infracciones penales. Nuestra duda es la forma de conjugar la confidencialidad de dichos datos (Artículo 10 de la ley de autonomía del paciente), así como la debida colaboración con las autoridades policiales.*

*Entendemos que dicha petición policial de datos personales sin consentimiento de las personas afectadas debe constar por escrito, consultando a dicha Agencia si deberá venir autorizada necesariamente por el órgano judicial correspondiente, o preferentemente, por suponer un modo más adecuado, formal y acreditable. En el supuesto de no precisarse orden judicial ¿en dicha petición si deben concretarse los documentos o datos y finalidad de su petición que sean precisos conocer para la investigación?.*

*Así mismo nos gustaría conocer que requisitos legales se establecen para la motivación y valoración de la necesidad para los fines de una investigación concreta para la investigación o represión de infracciones penales.*

*En relación al requerimiento en un Centro de Salud, nos surgen las siguientes cuestiones: ¿Qué procedimiento debe cursar la policía para solicitar datos personales o sanitarios de un paciente? ¿en qué casos consta la actuación de los agentes como policía judicial? ¿en qué casos la petición se debe formular mediante orden judicial, no siendo suficiente la petición por un agente policial?*

*En este sentido, también consultamos sobre los requisitos o condiciones especiales de protección de datos del Historial clínico, y garantía en la forma de la entrega a persona acreditada y en el uso que se de al mismo.*

*Disponiendo de un protocolo de seguridad y modelo de entrega de datos informatizados.*

*¿Qué requisitos deberían constar en un modelo de entrega de documentación con datos personales? ¿Deberíamos identificar a la solicitante en el modelo, así como en la extracción la finalidad y datos entregados?*

*Rogando que se nos de respuesta formal respecto a las consultas formuladas para concretar los supuestos actuales o futuros de petición de datos personales que XXXXX...”*

**SEGUNDO.** El artículo 17 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, en su apartado n) atribuye a esta Agencia la siguiente función:

*“Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta Ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta Ley.”*

Corresponde a esta Agencia Vasca de Protección de Datos, en virtud de la normativa más arriba citada, la emisión del informe en respuesta a la consulta formulada.



## CONSIDERACIONES

### I

Son varias las cuestiones planteadas en el escrito presentado por XXXXX de Osakidetza-Servicio Vasco de Salud, a las que intentaremos dar respuesta en el presente dictamen.

En primer lugar es necesario señalar que las cuestiones planteadas en la consulta están relacionadas con la cesión de datos personales por parte de los Centros de Salud a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado ante un requerimiento de los mismos.

A este respecto, se debe comenzar manifestando que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), conforma el marco jurídico de referencia que afecta a la protección de datos. En esta ley se regulan los principios y fundamentos a los que deben ajustarse la recogida y tratamiento de los datos personales por cualquier Institución que precise recabar este tipo de datos para el ejercicio de su actividad. Dicha Ley se complementa, en el ámbito de la Comunidad Autónoma Vasca, con la Ley 2/2004, de 25 de febrero, de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

La transmisión o cesión de datos a que se refiere la consulta constituye, desde el punto de vista de la LOPD una cesión de datos de carácter personal, definida en su artículo 3 i) como *“toda revelación de datos realizada a una persona distinta del interesado”*.

Estamos, por tanto, ante un supuesto de comunicación de datos, que con carácter general se regula en el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter General, donde se establece que la misma sólo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario y exige para que pueda tener lugar, el consentimiento del interesado (art.11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretende comunicar (art. 11.3).

No obstante, este régimen general de la comunicación de datos se encuentra excepcionado en los supuestos del apartado 2 del artículo 11:

*“2. El consentimiento exigido en el apartado anterior no será preciso:*

*a) Cuando la cesión está autorizada en una ley.*

*b) Cuando se trate de datos recogidos de fuentes accesibles al público.*

*c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En*



*este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.*

*d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.*

*e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*

*f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica”.*

Ahora bien, en cuanto a la recogida y tratamiento de datos de carácter personal para fines policiales por parte de las Fuerzas y Cuerpos de Seguridad, la LOPD establece una regulación específica en el artículo 22 de la misma, artículo que será examinado detalladamente a lo largo del presente informe.

## II

Señalado lo anterior, debemos de tener en cuenta que, en cuanto a la comunicación o cesión de datos de salud, la Ley Orgánica establece un régimen especial para su tratamiento y comunicación, considerándolos datos especialmente protegidos, debiendo plantearse si existe algún supuesto en que la propia Ley Orgánica de cobertura a esa cesión.

Así, en primer lugar, el artículo 7.3 de la LOPD dispone que “*los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente*”.

La especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal.

En este contexto, tanto el artículo 8 de la directiva 95/46/CE del Parlamento y del Consejo, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España el 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección.



Sin perjuicio de ello, el artículo 7 de la LOPD, en su número 6 determina:

*“No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.*

*También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento”.*

En segundo lugar, la LOPD también se refiere a los datos relativos a la salud dentro del artículo 8 bajo el epígrafe “datos relativos a la salud”, señalando expresamente:

*“Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con la legislación estatal o autonómica sobre sanidad”.*

Con relación a este precepto no existen demasiadas sentencias que se refieran al mismo y normalmente se analiza conjuntamente con el artículo 7. Así la Sentencia de la Audiencia Nacional de 12 de abril de 2002 señala:

*“El artículo 7 de la Ley 15/1999, al igual que su correlativo de la Ley anterior, configuran bajo la rúbrica de “Datos especialmente protegidos” un régimen especialmente cualificado, con protección más intensa, para aquellos datos personales que proporcionan una información de esferas íntimas del individuo. En concreto para los datos de salud (...) se considera que sólo pueden ser recabados, tratados o cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente (artículo 73 de la LORTAD y 7.3 de la LOPD). A pesar de lo anterior “(...) las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan ser tratados en los mismos, de acuerdo con la legislación estatal o autonómica sobre sanidad” (artículo 8). La ley anterior se refería específicamente a determinadas leyes sanitarias, pero en lo demás era exactamente igual a la vigente. La novedad se encuentra en el apartado 6 del artículo 7 que establece que “(...)”. A la luz de este precepto, el fundamento de la excepción de necesidad del consentimiento en el tratamiento de datos relativos a la salud se encuentra en la prevención, diagnóstico médico, prestación de asistencia sanitaria o tratamiento o la gestión de servicios sanitarios”.*

En tercer lugar, la LOPD también se refiere a los datos relativos a la salud dentro del artículo 11 dedicado a la comunicación de datos, en el apartado 2 dedicado a



excluir el consentimiento del interesado en ciertos casos, en concreto en la letra f) cuando señala:

*“Cuando la cesión de datos de carácter personal relativos a la salud sea necesario para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica”.*

En cuarto lugar, el artículo 22.3 de la LOPD, cuando se refiere a la recogida y tratamiento de datos de salud por las Fuerzas y Cuerpos de Seguridad, también establece una serie de restricciones, que serán examinadas posteriormente a lo largo del presente informe.

En quinto lugar, el artículo 34 c) establece una excepción a la regla general del artículo 33 sobre movimiento internacional de datos cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios. Aunque se refiere a todo tipo de datos personales y no menciona de forma expresa los datos de salud, parece evidente que éstos serán en la práctica los que tengan mayor relevancia a estos efectos.

Por último, la inclusión de los datos de salud en los ficheros comunes de las entidades aseguradoras, a que se refiere la Disposición Adicional Sexta de la LOPD no excluye de la necesidad del consentimiento, es decir, los datos referidos a la salud sólo podrán ser objeto de tratamiento con el consentimiento del afectado en relación con dichos ficheros.

### III

Dicho lo anterior, en cuanto a la diferencia en la cesión de datos personales en general y datos especialmente protegidos, como son los datos de salud, la presente consulta tendría por objeto el delimitar el alcance de la posible habilitación legal para la cesión de datos de carácter personal a los efectivos de las Fuerzas y Cuerpos de Seguridad del Estado que los solicitan en ejercicio de sus actividades, por lo que con carácter previo, deben analizarse las normas reguladoras, tanto de las Fuerzas y Cuerpos de Seguridad como de las funciones atribuidas a los miembros de la Policía Judicial, a los efectos de determinar el alcance de su actividad.

En este sentido, el artículo 1.4 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, señala que, *“el mantenimiento de la seguridad pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad”*, entre las que se incluyen, según artículo 2 de la propia Ley *“Las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la nación, los Cuerpos de Policía dependientes de las Comunidades Autónomas y los Cuerpos de Policía dependientes de las Corporaciones Locales”*.



Igualmente, conforme dispone el artículo 549.1 de la Ley Orgánica del Poder Judicial, tras la reforma operada por la Ley Orgánica 19/2003, de 23 de diciembre, *“corresponden específicamente a las unidades de Policía Judicial las siguientes funciones:*

- “a) La averiguación acerca de los responsables y circunstancias de los hechos delictivos y la detención de los primeros, dando cuenta seguidamente a la autoridad judicial y fiscal, conforme a lo dispuesto en las leyes.*
- b) El auxilio a la autoridad judicial y fiscal en cuantas actuaciones deba realizar fuera de su sede y requieran la presencia policial.*
- c) La realización material de las actuaciones que exijan el ejercicio de la coerción y ordenare la autoridad judicial y fiscal.*
- d) La garantía del cumplimiento de las órdenes y resoluciones de la autoridad judicial o fiscal.*
- e) Cualquier otras de la misma naturaleza en que sea necesaria su cooperación o auxilio y lo ordenare la autoridad judicial o fiscal”.*

Del transcrito precepto se desprende que, junto con las funciones encomendadas a la Policía para el cumplimiento de las actuaciones ordenadas por la Autoridad Judicial o el Ministerio Fiscal, existen otras, directamente dirigidas a la averiguación de las actuaciones delictivas y detención de los presuntos responsables, que se llevan a cabo con carácter previo a la iniciación del correspondiente proceso penal, siendo la finalidad de estas últimas la determinación de los elementos de convicción precisos para que pueda proceder esa iniciación, siendo obligación de la Policía poner los hechos en inmediato conocimiento de la Autoridad judicial o del Ministerio fiscal.

En lógica correlación con ello, el artículo 2 del Real Decreto 769/1987, de 19 de junio, regulador de la Policía Judicial, establece que *“los miembros de las Fuerzas y Cuerpos de seguridad, en sus funciones de Policía Judicial, desarrollarán los cometidos expresados en el artículo 1, a requerimiento de la Autoridad judicial, del Ministerio Fiscal o de sus superiores policiales o por propia iniciativa a través de estos últimos, en los términos previstos en los artículos siguientes”.* En este mismo sentido, añade el artículo 4 del citado Real Decreto que *“ todos los componentes de las Fuerzas y Cuerpos de Seguridad, cualquiera que sea su naturaleza y dependencia, practicarán por su propia iniciativa y según sus respectivas atribuciones, las primeras diligencias de prevención y aseguramiento así que tengan noticia de la perpetración del hecho presuntamente delictivo, y la ocupación y custodia de los objetos que provinieren del delito o estuvieren relacionados con su ejecución, dando cuenta de todo ello en los términos legales a la Autoridad Judicial o Fiscal, directamente o a través de las Unidades Orgánicas de la Policía Judicial”.*

#### IV

A la vista de lo anterior, y para dar respuesta adecuada a la consulta planteada, se debe distinguir, por una parte aquellas actuaciones de las Fuerzas y Cuerpos de Seguridad 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 un superior jerárquico; y por otra, la



tipología de datos solicitados, sean éstos especialmente protegidos (datos de salud) o no.

Respecto de las actuaciones de la Policía que son llevadas a cabo en cumplimiento de un mandato judicial, hay que partir de la consideración de que 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 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.

Por ello, es necesario determinar el régimen aplicable a la cesión de datos a Jueces y Tribunales, distinguiendo entre los distintos tipos de datos a que se refiere la consulta:

a) en cuanto a los datos personales que no son especialmente protegidos: resultaría de aplicación directamente el artículo 11.2 d) de la LOPD que determina que no será necesario el consentimiento del interesado:

*“Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.”*

b) Respecto de los datos especialmente protegidos, esto es, datos de salud es preciso recordar, como hemos señalado anteriormente, que la LOPD establece un sistema de protección especial, no siéndole de aplicación el artículo 11.2 d) dado su especial carácter. A este respecto se debe tener en cuenta que los datos relativos a la salud son una información especialmente sensible que, por su importancia y naturaleza, forman parte del derecho a la intimidad y privacidad y que este derecho resulta afectado cuando se accede a los mismos sin consentimiento del interesado. Ahora bien, la falta de consentimiento, por si sola, no implica directamente la eventual vulneración del derecho. En efecto, como otros derechos, el derecho a la intimidad no constituye un derecho absoluto, y puede ceder frente a otros siempre que concurren determinadas condiciones por lo que sería de aplicación el artículo 7.3 de la LOPD cuando señala:

*“Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente”.*

En relación con dicho precepto, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, establece que la Historia Clínica tiene por fin principal facilitar la asistencia sanitaria, recogiendo todos los datos, que bajo criterio médico, permitan el conocimiento veraz y actualizado de su estado de salud., pero señalándose igualmente en su artículo 16 apartado 3 que:



*“3. El acceso a la historia clínica **con fines judiciales**, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de **investigación de la autoridad judicial** en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, **en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente**. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.”*

Por tanto, en lo que se refiere al acceso a la historia clínica por parte de la autoridad judicial o del ministerio fiscal, se establecen dos limitaciones:

- El acceso para fines judiciales: deberán someterse a una previa disociación de los datos contenidos en la historia clínica, de manera que como regla general quede asegurado el anonimato, a menos que el interesado haya prestado su consentimiento para ello en los términos del artículo 7.3 de la LOPD.
- Si el acceso se solicita por una autoridad judicial y la identificación del paciente es necesaria para la tramitación del proceso en que los datos se solicitan: se estará a los términos de la correspondiente Resolución Judicial, quedando el acceso limitado estrictamente a los fines específicos de cada caso.

Por tanto, el acceso a los datos sanitarios se podrá llevar a cabo, sin vulneración de la normativa sobre protección de datos, siempre que se cumplan las condiciones y requisitos establecidos en la norma sectorial que regula dicho acceso, es decir, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

## V

Procede ahora analizar el régimen aplicable a aquellos supuestos en que las actuaciones de la Policía se llevan a cabo por propia iniciativa o a instancia de un superior jerárquico y no existe mandamiento judicial.

A este respecto, el artículo 22.2 de la LOPD, relativo a ficheros de las Fuerzas y Cuerpos de Seguridad determina:

*“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.”*

Estableciendo así mismo, el artículo 22 en su párrafo 3º respecto de los datos relativos a la salud, es decir, los datos especialmente protegidos que:

*“La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales”.*

La especialidad de la recogida de datos sin consentimiento del titular por parte de la Policía deriva de la actividad de investigación policial reconocida a las Fuerzas y Cuerpos de Seguridad en la Ley Orgánica 2/1986, sobre Fuerzas y Cuerpos de Seguridad del Estado (artículo 11), plasmación del mandato constitucional de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, recogido en el artículo 104 de la Carta Magna.

Por tanto, el artículo 22 habilitaría, a nuestro juicio, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, a recabar y tratar datos de carácter personal sin consentimiento de los afectados únicamente cuando se cumplan los requisitos mínimos de proporcionalidad exigidos, como así ha sido declarado tanto por esta Agencia de Protección de Datos en su informe CN09-016, como en reiterados informes de la AEPD, entre ellos en el 0133/2008 , en el 0169/2009, o en el más reciente 0086/2010.

Reproducimos, por ser de interés, parte del informe CN 09-016 de esta Agencia Vasca de Protección de Datos:

*“...Si bien es cierto que la investigación policial requiere una intervención rápida, y por lo tanto, el responsable del fichero no debe entrar en un análisis pormenorizado de la petición de datos, sí que al menos debe comprobar que dicha petición cumple unos requisitos mínimos de proporcionalidad. Es la propia Jefatura Provincial de Policía quien en su segundo escrito hace mención al informe jurídico 0133/2008 de la Agencia Española de Protección de Datos, el cual, reitera los criterios señalados en otro informe anterior de 1999, a tener en cuenta a la hora de ceder datos solicitados por la Policía al amparo del artículo 22.2 de la LOPD.*

*Reproducimos a continuación parte de dicho informe:*

*“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 la Policía Judicial, cumpla las siguientes condiciones, que han sido reiteradas por la Agencia Española de Protección de Datos:*

*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”.*

*Téngase en cuenta que estos requisitos que a juicio de la Agencia Española de Protección de Datos debe reunir la petición no se refieren a los datos a mencionados en el 22.3, sino a los del 22.2, esto es, no es preciso que se trate de una solicitud de datos especialmente protegidos (ideología, religión, creencias, afiliación sindical, vida sexual, raza, salud). La petición de cualquier otro dato de carácter personal debe de cumplir las exigencias antes citadas.*

*En el mismo sentido se ha posicionado la doctrina, siendo conveniente citar a este respecto a Troncoso Reigada, que, en su manual de protección de datos para Administraciones Locales, al comentar la cesión de datos del Padrón Municipal a la policía, señala lo siguiente:*

*“Por tanto, se puede afirmar que las Fuerzas y Cuerpos de Seguridad tienen una habilitación legal específica para obtener información de datos personales, incluidos los datos del Padrón Municipal. La propia LOPD incluye la previsión legal exigida en el art. 11.2.a) de la LOPD, estableciendo una referencia específica en el art. 22 de la LOPD para las Fuerzas y Cuerpos de Seguridad en atención a los bienes jurídicos en presencia. En todo caso, la comunicación de datos a las Fuerzas y Cuerpos de Seguridad del Estado tiene unos requisitos que serían: que se acredite que la obtención de datos del padrón es necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales; y que se trate de una petición concreta y específica de la que quede constancia, hecha por persona con autoridad para ello, de manera motivada, donde se acredite que la petición encaja con lo previsto en la ley. No parece claro que la LOPD prohíba las solicitudes amplias de datos del Padrón, siempre que sean necesarias para la prevención de los delitos o la persecución de infracciones penales y que éstas estén motivadas. Además, no parece muy razonable que el responsable del Padrón pueda obtener una información muy detallada sobre la finalidad para la que se solicitan los datos. No obstante, el requisito legal es claro y se refiere exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, lo que no es una habilitación vacía o sin contenido. La prudencia en la petición y en la resolución le corresponde a las dos partes implicadas.”*

*Resulta lógica esta prevención, así como coherente con las previsiones del ordenamiento jurídico, pues en los casos en que se permiten accesos masivos a datos personales por parte de la policía, existe una previsión legal expresa. Así, la Ley Orgánica 14/2003, de 20 de noviembre, modifica la Ley de Bases de Régimen Local al añadir la Disposición Adicional Séptima, cuyos dos primeros párrafos pasamos a transcribir:*

*“Para la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley Orgánica de derechos y libertades de los extranjeros en España y su integración social, sobre control y permanencia de extranjeros en España, la*



*Dirección General de la Policía accederá a los datos de inscripción padronal de los extranjeros existentes en los Padrones Municipales, preferentemente por vía telemática.*

*A fin de asegurar el estricto cumplimiento de la legislación de protección de datos de carácter personal, los accesos se realizarán con las máximas medidas de seguridad. A estos efectos, quedará constancia en la Dirección General de la Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados.”*

*Como vemos, el instrumento normativo para habilitar el acceso a gran cantidad de datos incluidos en el Padrón, no es el artículo 22.2, sino que se acude a una previsión legal específica. Otra muestra de este criterio la encontramos en la Ley Orgánica 1/1992, de 21 de febrero, cuyo artículo 12 señala lo siguiente:*

*“Las personas naturales o jurídicas que desarrollen actividades relevantes para la seguridad ciudadana, como las de hospedaje, el comercio o reparación de objetos usados, el alquiler o el desguace de vehículos de motor, o la compraventa de joyas y metales preciosos, deberán llevar a cabo las actuaciones de registro documental e información previstas en la normativa vigente”.*

*Esta Ley cuyo fundamento último se encuentra en el Convenio de Schengen, ha sido considerada como norma habilitante por parte de la Agencia Española de Protección de Datos (Informe 152/2003), para excepcionar en la cesión de estos datos a la Policía, la necesidad de consentimiento del titular. Parece por tanto que el criterio en el acceso masivo a datos de carácter personal sea la necesidad de una previsión legal específica y diferente a la recogida en el artículo 22.2 de la LOPD...”*

Por tanto, a la vista de lo anteriormente referenciado, no cabe duda que, por parte del cedente, se debe de constatar inequívocamente, que se cumplen 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”.

Dichas condiciones, como se ha destacado anteriormente, se exigen para la cesión de todo tipo de datos, sean o no especialmente protegidos, debiendo destacarse que la mayor protección que establece la normativa en cuanto a los datos especialmente protegidos, como son los datos de salud, ha dado lugar a que el propio artículo 22.3



de la LOPD, anteriormente transcrito, disponga también un régimen reforzado de protección para el supuesto de que las Fuerzas y Cuerpos de Seguridad recojan o traten los datos especialmente protegidos o sensibles, como son en este caso los datos de salud.

Este régimen reforzado exige que la recogida y tratamiento de datos de salud se haga sólo cuando sea absolutamente necesario para los fines de una investigación concreta, y sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. Este extremo deberá igualmente quedar suficientemente acreditado en la solicitud formulada.

## VI

De acuerdo con lo manifestado anteriormente, y en cuanto a al resto de las cuestiones planteadas por XXXXX de Osakidetza-Servicio Vasco de Salud, compartimos el criterio de la misma de la necesidad de que quede constancia de la solicitud formulada por las Fuerzas y Cuerpos de Seguridad, que deberá contener los requisitos señalados en el apartado anterior del presente informe, y cuando actúe con mandamiento judicial deberá quedar constancia de dicho mandamiento.

Asimismo, el órgano cedente deberá poder acreditar qué datos ha cedido, en qué fecha y a quién y si la cesión realizada obedece a la solicitud formulada, una vez ponderados los requisitos, principios y garantías exigidos por la LOPD.

Respecto a la cuestión sobre si la petición se debe formular mediante orden judicial, es una decisión que escapa a la competencia de esta Agencia, recordándole que, como se ha señalado en el presente informe, la LOPD habilita la cesión de datos a las Fuerzas y Cuerpos de Seguridad, siempre que se cumplan las condiciones señaladas en el mismo, tanto cuando existe mandamiento judicial, como en aquellos casos que, no existiendo el mismo, se dan las condiciones para efectuar la cesión.

En cuanto a la valoración de la necesidad de los datos recabados para la investigación o represión de infracciones penales, nada puede decir esta Agencia al respecto, ya que lo contrario supondría una intromisión en las facultades de decisión que competen en exclusiva al cedente, debiendo ser él mismo el que realice dicha valoración, caso a caso, a la vista de las circunstancias concurrentes y atendiendo a las recomendaciones señaladas anteriormente, resolviendo si se cumplen o no los requisitos legales para hacer efectiva la cesión y el modo de realizar la misma, pero teniendo en cuenta, en cualquier caso, que aun en los supuestos en que el tratamiento de datos cuente con habilitación legal habrá de aplicar el principio de calidad de datos recogido en el artículo 4 de la LOPD de acuerdo con el cual:

*“Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.”*



Este principio implica someter los tratamientos de datos a un criterio de racionalidad a fin de que sólo aquellos datos que resulten adecuados, pertinentes y no excesivos sean objeto de tratamiento.

## **CONCLUSIÓN**

La cesión de datos de carácter personal a los miembros de las Fuerzas y Cuerpos de Seguridad, no vulneraría la normativa en materia de protección de datos de carácter personal, siempre que se cumplan las condiciones apuntadas en el cuerpo del presente informe.

En Vitoria-Gasteiz, a 2 de febrero de 2011