Procedimiento nº.: PS/00157/2011

ASUNTO: Recurso de Reposición Nº RR/00740/2011

Examinado el recurso de reposición interpuesto por la entidad MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00157/2011, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 26 de septiembre de 2011, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00157/2011 , en virtud de la cual se imponía a la entidad denunciada, una sanción de 40.001 €, por la vulneración de lo dispuesto en el artículo 9.1de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como grave en el artículo 44.3.h), de conformidad con lo establecido en el artículo 45.2.4 y .5 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 29 de septiembre de 2011, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00157/2011, quedó constancia de los siguientes:

<< *PRIMERO:* *El denunciante ha declarado que con fecha 16 de septiembre de 2009, con motivo de su incorporación laboral a la entidad Mutua General de Cataluña, se realizó un reconocimiento médico cuyos resultados fueron trasladados al departamento de RR.HH de la citada entidad. En este reconocimiento le realizaron la prueba de VIH con resultado positivo. Manifiesta que él no autorizó que se le realizase la citada prueba y tampoco le fue entregada una copia del Informe con el resultado del reconocimiento practicado.*

El denunciante solicitó tanto a la clínica Cruz Blanca, donde le hicieron el reconocimiento, como a Mutua General, copia de toda la documentación médica, protocolo para la realización de las pruebas, y el documento firmado donde constase el consentimiento informado de la prueba del VIH, a lo que las entidades contestaron que no tenían ningún documento firmado. (folios 1 a 41)

SEGUNDO: *El 3 de noviembre de 2010, se realizó una inspección en la entidad CENTRO DE EXÁMENES MÉDICOS, S.A. (Centro Médico Creu Blanca), poniéndose de manifiesto los siguientes hechos:*

CENTROS MÉDICOS CREU BLANCA, es una marca comercial en la que se integran diversas entidades, entre las que se encuentra CENTRO DE EXAMENES MEDICOS, S.A y el INSTITUTO CLÍNICO DE ALTA TECNOLOGÍA, S.A., el cual suscribió un contrato de prestación de servicios médicos con la empresa MUTUA GENERAL DE CATALUÑA, con fecha 17 de septiembre de 1996, renovado con fecha 28 de noviembre de 2002.

Los servicios contratados por MGC, consisten en la elaboración de historia clínica de los trabajadores que son remitidos por la misma, exploración médica, agudezas visuales y auditivas, electrocardiogramas, RX, de tórax, analítica de sangre y orina, Informe de conclusiones, además se pactó la prueba de HIV añadida a la analítica. Desde el año 1996, MGC remite puntualmente a la Clínica Creu Blanca trabajadores para la realización de reconocimientos médicos, a los cuales se les realizan todas las pruebas contratadas. (folios 42 a 58)

TERCERO: *La representante de la entidad inspeccionada el 3 de noviembre de 2010 manifiesta que al detectarse que la prueba del VIH del denunciante había resultado positiva, el Gerente del Centro se puso en contacto telefónico con el Director médico de MGC, para consultar si se realizaba una confirmación, a lo que el MGC contestó que se realizase.*

El 28 de septiembre de 2009 una vez confirmada la prueba de VIH, se remitió a MGC toda la documentación del Sr. ***B.B.B.*** *resultado del chequeo y la analítica completa.*

Con fecha 31 de marzo de 2010 el interesado solicitó a esta Clínica el acceso a su expediente. Con fecha 8 de abril de 2010 se le hace entrega de copia de toda la información contenida en el mismo, cuando el interesado se persona en la Clínica para su recogida. Con relación al consentimiento para la prueba de HIV, con fecha 12 de abril se le informa telefónicamente de que no existe ningún documento firmado.

La representante de la entidad manifiesta que a todos los trabajadores remitidos por MGC se les practican las mismas pruebas, incluido el VIH, no obstante no se les solicita el consentimiento escrito del trabajador, a pesar de que siempre que se practica dicha prueba a cualquier otro colectivo, es imprescindible dicho requisito. (folios 42 a 58)

CUARTO*: El 13 de diciembre de 2010 se realiza inspección en la entidad MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA, poniéndose de manifiesto los siguientes hechos:*

Todos los resultados de las pruebas realizadas a los trabajadores son remitidos a MGC por Centros médicos Creu Blanca en un sobre cerrado que se entrega en

mano al Director Médico de la entidad. No obstante, éste solo se pone en contacto con el trabajador en los casos en que aparece alguna anomalía no conocida por éste y que deba ser tratada médicamente. Todos los resultados de los reconocimientos médicos recibidos en MGC son custodiados en la Caja fuerte de la entidad, a la que solo tienen acceso el Director General y el Director General Adjunto.

MGC tiene suscrito un contrato de prestación de servicios de Prevención de Riesgos Laborales con la empresa GENARS, S.L., no obstante dicha entidad solo se encarga de los reconocimientos médicos periódicos que se realizan a todos los trabajadores de la empresa que lo desean.

En el mes de marzo de 2009 MGC decidió contratar al denunciante de este procedimiento.

Con relación a los citados reconocimientos el Director médico de la entidad, manifiesta que el procedimiento seguido es el siguiente:

Cuando un trabajador va a formar parte de la plantilla, desde el Departamento de RR.HH. se le informa que se le va a realizar un reconocimiento médico previo a su incorporación y se le remite al Centro Creu Blanca para su realización.

Una vez conocidos los resultados de reconocimiento al denunciante en este procedimiento, el Director médico de MGC se lo comunica al Director General Adjunto, quien manifiesta no ser conocedor de que fuera seropositivo, por lo que el Director médico, siguiendo el protocolo establecido en la entidad, procede a informar al interesado sobre el resultado de la analítica. (folios 59 a 65)

QUINTO: *Los representantes de MGC han manifestado que no cuentan con documentación suscrita por el interesado otorgando el consentimiento para la realización de la prueba de VIH, hecho por el que no le fue remitida al mismo tras su solicitud de fecha 16 de abril de 2010.*

Se comprueba por los inspectores de esta Agencia, que en la caja fuerte de MGC hay varias estanterías con el anagrama del Centro médico Creu Blanca, que según manifiesta el representante de la entidad, corresponden a los informes médicos de cada uno de los trabajadores. Se comprueba que uno de ellos es el relativo al denunciante, con los resultados de las pruebas realizadas y entre ellas la analítica. (folios 59 a 65)>>

TERCERO: MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA ha presentado en fecha 13 de octubre de 2011, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en
"Queda claro que la Agencia en su Resolución está sancionando a la recurrente por el riesgo de acceso por personas distintas al Director Médico, pero no por el acceso real (único sancionable) de los Directores Generales a los informes médicos del denunciante, hecho que no se ha producido ni, lógicamente, se ha probado. (...)

De todo lo expuesto, podemos concluir que no se ha producido ningún acceso no autorizado y que en ningún caso se ha probado el mismo. La Agencia deduce un riesgo no un resultado de las medidas de seguridad adoptadas por la recurrente. Las medidas

pueden mejorarse pero en ningún caso han resultado ineficaces. (...)
Dicha Sentencia declara algo que resulta evidente y es que la vulneración de la obligación de secreto exige revelar la información confidencial a un tercero. La Audiencia Nacional, como hemos señalado y probado anteriormente, ha calificado reiteradamente (Sentencias de 28 de junio de 2006, 11 de diciembre de 2008 y 25 de febrero de 2010) la obligación contenida en el artículo 9.1 de la LOPD como una obligación de resultado, compartiendo la misma naturaleza obligacional del artículo 10 de la LOPD. La diferencia entre ambas obligaciones es que mientras el deber de secreto implica que la información no sea revelada a terceros, la obligación de adoptar medidas de seguridad implica que estas hayan sido adoptadas y se revelen eficaces, eficacia que se presumirá mientras no se pruebe la pérdida, extravío, tratamiento o acceso no autorizado. (...)
No encuentra la Agencia ningún motivo de exoneración de responsabilidad, cuando, como ha quedado demostrado, no se ha aportado ninguna prueba de pérdida, extravío, tratamiento o acceso no autorizado, conforme exige una obligación de resultado, y así ha sido calificada la obligación del artículo 9 por la Audiencia Nacional.(...)
A esas declaraciones habría que añadir la inexistencia de pérdida, extravío, tratamiento o acceso no autorizado por parte de tercero, pues la Agencia sanciona por permitir "que los datos personales fueran accesibles por terceros no autorizados" (rio porque se hubiera accedido realmente a ellos)."

Con fecha 20 de octubre de 2011, la recurrente presenta escrito donde en síntesis expone:

"La Agencia en su Resolución da a entender que la Mutua puede mejorar sus medidas de seguridad con objeto de evitar riesgos de acceso no autorizado. Esa recomendación que se deduce de la Resolución recurrida, ha sido debidamente tomada en consideración por la Mutua, quien ha dispuesto dentro de la cámara acorazada un archivo metálico de seguridad con una llave que se ha entregado al Director Médico, Dr. ***A.A.A.****, para su custodia. (...) SOLICITA tenga por presentado este escrito complementario al recurso de reposición, y se tenga por informada de la adopción de nuevas medidas de segundad."*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC).

II

En relación con las manifestaciones efectuadas por MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA, reiterándose básicamente, en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del VI al C.C.C. ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

*<< **VI***

El artículo 9 de la LOPD dispone lo siguiente:
"1. El responsable del fichero, y, en su caso, el encargado del tratamiento,

deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Para poder delimitar cuáles son los accesos que la Ley pretende evitar, exigiendo las pertinentes medidas de seguridad, es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

En lo que respecta al concepto de "fichero" el artículo 3.b) de la LOPD lo define como "todo conjunto organizado de datos de carácter personal", con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la "comunicación" o "consulta" de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Sintetizando las previsiones legales citadas puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca, están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, regulado en normas reglamentarias.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define en su artículo 5.2 ñ) el "Soporte" como el "objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos".

Por su parte el artículo 81.1 del mismo Reglamento señala que "Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico". Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104. El artículo 88, en su punto 3, referido al documento de seguridad, establece lo siguiente:

"El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos".

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. En el caso que nos ocupa, como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

De los hechos probados en este procedimiento, se deduce que MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA, en su calidad de responsable del tratamiento de los datos de salud contenidos en los resultados de las pruebas analíticas de sus empleados, debió adoptar las medidas necesarias para impedir cualquier acceso a la información de carácter personal que contenía dicha documentación. Tales medidas no fueron adoptadas totalmente en el presente caso, como lo acredita el hecho constatado en el acta de inspección de 13 de diciembre de 2010, de que los resultados de los reconocimientos médicos de los trabajadores de MGC son custodiados en la caja fuerte de la entidad a la que tienen acceso el Director médico y el Director General Adjunto, comprobándose que entre los informes se encuentra el correspondiente al denunciante de este procedimiento con los resultados de las pruebas realizadas entre las que se encuentra la analítica de VIH. Por otra parte en las alegaciones al acuerdo de inicio de este procedimiento, el representante de Mutua manifiesta que, además del Director médico de la entidad, el acceso a la cámara acorazada en que se custodian los informes médicos de los trabajadores "está limitado al Director General de la entidad, ... que, igualmente es médico, y a los dos Directores Generales Adjuntos, todos ellos sujetos al deber de confidencialidad".

Esta necesidad de especial diligencia en la custodia de la documentación por el responsable del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11 de diciembre de 2008 (recurso 36/08), fundamento cuarto: "Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".

El artículo 5.1.g) del Reglamento de la LOPD dispone que se entenderá por "datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética."

No hay duda de que el acceso a los resultados de los informes médicos de los trabajadores del MGC por personas que no pertenecen al servicio médico de la empresa, lleva a la conclusión de que las medidas de seguridad no evitaron el acceso de personas no autorizadas a los datos de carácter personal relacionados con la salud.

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido, la profesionalidad exigible al infractor. En este sentido la Sentencia de 5 de junio de 1998 exige a los profesionales del sector "... un deber de conocer especialmente las normas aplicables".

Se ha alegado al acuerdo de inicio del expediente sancionador, que "Los expedientes médicos, ... se guardan y custodian en una cámara acorazada (caja fuerte) ubicada en la sede social de la MGC, cuyo acceso está limitado al Director General de la entidad, ... que, igualmente es médico, y a los dos Directores Generales Adjuntos, todos ellos sujetos al deber de confidencialidad. (...)
Pero no sólo se guardan los expedientes en un espacio físico que reúne las características adecuadas para garantizar la confidencialidad de la información (cámara acorazada) y se limita el acceso al mismo a personas físicas concretadas e identificadas, que, por su responsabilidad, están sujetas al deber de confidencialidad, sino que además existe un protocolo de acceso que impide que ninguna otra persona pueda abrir la cámara de seguridad, pues únicamente los tres Directores Generales disponen de las tarjetas de acceso, con un código de entrada personalizado que lo permite. (...)
Parece claro que las medidas de seguridad que ha adoptado MGC para preservar la confidencialidad de los expedientes médicos cumple con la normativa y con el criterio sentado por la AEPD. Una cámara acorazada que es exactamente lo que es la caja fuerte a la que nos venimos refiriendo, con un acceso limitado a los máximos

representantes de la entidad, quienes disponen de tarjetas de acceso específicas y programadas que únicamente les permiten el acceso a dicha cámara a ellos tres y a ninguna otra persona supone la adopción de medidas de seguridad de un alto nivel de control de accesos y unas medidas que tecnológicamente no pueden ser vulneradas."

Con fecha 5 de julio tiene entrada en esta Agencia un escrito de MGC en el que manifiesta que los hechos recogidos en el acta de inspección practicada por esta Agencia puede llevar a error si no se aclaran determinados conceptos. En concreto MGC aclara lo relativo al acceso a la caja acorazada, en que se guardan los informes médicos de los trabajadores, diciendo que las personas que no forman parte del servicio médico y que tienen acceso a la caja en que se guardan los informes no tienen autorización para acceder a los informes, que está limitado al director médico. Que la razón de esto es que la cámara acorazada es el lugar más seguro de toda la Mutua donde se guardan otros documentos confidenciales, y que están completamente separados y en espacios bien diferenciados.

Se expone en este escrito también lo relativo a los deberes de diligencia, lealtad, secreto profesional y confidencialidad de los directores generales, el historial de la Mutua en el cumplimiento de los deberes de la LOPD, el proceso de recepción de los resultados médicos, el caso concreto de la denuncia y por último la actuación del denunciante ante la jurisdicción laboral. Esto último dirigido a explicar que, al parecer, "la actuación de denunciante obedece a una estrategia jurídica dirigida a obtener por vía laboral una indemnización."

Lo alegado en este escrito viene a complementar lo constatado en el acta de inspección de 13 de diciembre de 2010 y lo manifestado en las alegaciones al acuerdo de inicio de este procedimiento sancionador, y no modifica lo probado hasta el momento, el acceso a datos de salud de los trabajadores de MGC por personal no perteneciente al servicio médico de la entidad, que no puede negarse en un segundo escrito basándose en que tienen acceso pero no autorización y que el motivo de esta situación es que la caja fuerte es el lugar más seguro de la empresa.

Por otra parte cabe desestimar el resto de cuestiones planteadas en este escrito tales como que las especiales circunstancias de este caso permiten interpretar los artículos 11.2.c y 7.6 de la LOPD en el sentido de que el consentimiento exigido para la cesión de datos no era necesario porque se trataba de solucionar una urgencia. También cabe desestimar la alegación de que el tratamiento de datos personales puede realizarse por "otra persona sujeta a una obligación de secreto" cuando sea necesario para la prevención, diagnóstico médicos, prestación sanitaria, tratamientos médicos o gestión de servicios sanitarios. Y esto porque ninguna de estas situaciones se daban en el presente caso, que se encuadra dentro de una práctica propia de la entidad imputada, de realización de reconocimientos médicos previos a la incorporación a la plantilla y no se trataba de una urgencia médica que permitiera cesión de datos inconsentida, ni eximía del consentimiento para el tratamiento de datos porque fuera necesario para prevención, diagnóstico, prestación o tratamiento médico. Por todo ello cabe desestimar lo alegado.

En las alegaciones a la propuesta de resolución respecto de esta cuestión se expresa "Lo que se quiso decir es que la posibilidad de que los Directores Generales

pudieran en determinadas circunstancias de urgencia (por ejemplo, salvar los expedientes en caso de incendio o inundación) acceder a los historiales médicos estaría justificada en la propia LOPD. Es decir, el hecho de que puedan acceder a la cámara acorazada no es "per se" sancionable, pues la propia LOPD recoge supuestos en que los Directores Generales estarían autorizados por Ley a acceder a los expedientes médicos". En primer lugar en esta ocasión la infracción que se imputa no es la de cesión de datos y por otra parte, la interpretación que se hace de la expresión "solucionar una urgencia" no se corresponde con la que la LOPD establece en su artículo 11.2.f) que se refiere, como ya dijimos, a urgencias médicas por más que se intenten explicar otras circunstancias de urgencia posibles.

Resulta así probado que los datos personales relativos a la salud de los trabajadores de MGC son accesibles a personas que no pertenecen al servicio médico de la entidad que son los únicos que necesitan utilizar esta información para el desarrollo de sus funciones. Sobre esta cuestión el artículo 91 del Reglamento de desarrollo de la LOPD establece, con relación al control de accesos, lo siguiente:

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Este artículo 91 del RD 1720/2007, se encuentra entre las medidas de seguridad de nivel básico aplicables a tanto a ficheros y tratamientos automatizados como a los no automatizados.

También el artículo 113 de este Real Decreto, respecto de ficheros y tratamientos no automatizados entre las medidas de seguridad de nivel alto, referido al acceso a la documentación, expresa lo siguiente:

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

En este caso concreto, los informes médicos del personal de MGC son accesibles por personas ajenas al servicio médico de la empresa. A este respecto podemos ver quien está capacitado para acceder a esta información. El artículo 22.4 de

la Ley 31/1995, de Prevención de Riesgos Laborales expresa:

"Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador.

El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.

No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva."

El acceso a estos datos de salud debe limitarse al personal médico con funciones de vigilancia de la salud de los trabajadores y no puede facilitarse a otras personas sin conocimiento expreso del trabajador. Esto unido a las medidas de seguridad exigidas en la LOPD con relación al acceso a los usuarios únicamente a los recursos que precisen para el desarrollo de sus funciones implantando un control en el que se establezcan los mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados, lleva a concluir que se ha vulnerado por parte de MGC el principio de seguridad de los datos.

En esta cuestión podemos recordar lo que expresa el Tribunal Constitucional en su sentencia 196/2004, de 15 de noviembre de 2004: "El reconocimiento médico en la relación laboral no es, en definitiva, un instrumento del empresario para un control dispositivo de la salud de los trabajadores, como tampoco una facultad que se le reconozca para verificar la capacidad profesional o la aptitud psicofísica de sus empleados con un propósito de selección de personal o similar. Su eje, por el contrario, descansa en un derecho del trabajador a la vigilancia de su salud ... En suma, la regla es ... la conformidad libre, voluntaria e informada del trabajador para la vigilancia y protección de su salud frente a los riesgos del trabajo."

La MGC ha alegado a la propuesta de resolución que al no tratarse de las pruebas a las que se refiere la Ley de Prevención de Riesgos Laborales, no son aplicables las limitaciones de acceso establecidas en ella, ni tampoco la sentencia del Tribunal Constitucional 196/2004. Esta Ley se considera plenamente aplicable. En su artículo 3, sobre el ámbito de aplicación expresa que esta Ley y sus normas de desarrollo serán de aplicación tanto en el ámbito de las relaciones laborales reguladas en el texto refundido de la Ley del Estatuto de los Trabajadores...Con relación a la Sentencia del Constitucional mencionada, ya se ha contestado a lo alegado en el Fundamento de Derecho II de la presente Resolución.

La Audiencia Nacional, en varias sentencias, entre otras las de fechas 14 de febrero y 20 de septiembre de 2002 y 13 de abril de 2005, exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que

los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

En las alegaciones a la propuesta de resolución se manifiesta por MGC que "para el Juzgado de lo Social es un hecho probado que el Sr. ***B.B.B.*** *conoció las pruebas y prestó su consentimiento". Hay que decir de nuevo que la infracción imputada en este caso se refiere a las medidas de seguridad y no se cuestiona la existencia de consentimiento, pero en todo caso esta afirmación no se corresponde con lo expresado en la Sentencia nº 172/2011 del Juzgado de lo Social nº 31 de Barcelona que se menciona, toda vez que en toda su extensión no se recoge dicho "hecho probado" y en concreto en su Fundamento de Derecho Cuarto podemos leer: "En este caso lo probado es diferente de lo afirmado en la demanda. Se ha probado que el actor fue objeto de unas pruebas médicas para las que no prestó un consentimiento expreso, y que de ellas resultó el conocimiento por el director médico de la entidad de que el actor era portador del VIH. Como elemento relevante probado adicionalmente puede añadirse que a tales pruebas, con idéntico protocolo, eran (al menos en aquel momento) sometidos todos los nuevos empleados de la compañía, sin suscribir un consentimiento expreso al efecto."*

La Mutua declara en sus alegaciones a la propuesta de resolución que "la infracción requiere que se dé un resultado (y por tanto no se cumple el tipo sancionador -las obligaciones de resultado exigen que se dé el resultado-), aún en el supuesto de que la infracción lo fuera de riesgo (equiparándola a los delitos de riesgo), la realidad es que no se ha producido ningún acceso por persona no autorizada".

Sobre esta cuestión cabe decir que la infracción imputada es la falta de medidas de seguridad que como la Audiencia Nacional ha expresado en múltiples ocasiones (entre ellas la Sentencia de 7 de mayo de 2009 recurso n. 471/2008*), es una infracción de actividad que no exige la puesta en conocimiento de un tercero de los datos personales que sería la alegada infracción de resultado que no es la infracción atribuida en el presente caso. La infracción de resultado es la prevista en el artículo 10 LOPD la vulneración del deber de secreto, que sí exige el resultado de la puesta en conocimiento de los datos personales a tercero, mientras que en este procedimiento se imputa la infracción prevista en el artículo 9 de la LOPD.*

VII

El artículo 44.3.h) tipifica como infracción grave la siguiente:

"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"

En el presente caso ha quedado acreditado que MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA carecía de las medidas de seguridad que la Ley exige al responsable del fichero, al permitir el acceso a terceras personas no autorizadas a los resultados de los informes médicos de sus

trabajadores.

De acuerdo con los fundamentos anteriores, se deduce que por parte de MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA se ha producido una vulneración del principio de seguridad de los datos, que ha tenido como consecuencia que los datos personales de sus trabajadores fueran accesibles a terceros no autorizados, infracción que procede calificar como grave, sin que pueda exonerarse su responsabilidad tal como se ha demostrado en este procedimiento, por lo que procede su imputación, elemento necesario en el derecho administrativo sancionador tal como establece la STS de 27/5/99: "Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo".

Solicita MGC en las alegaciones al acuerdo de inicio y a la propuesta de resolución, que se adopte acuerdo de recomendación o apercibimiento. La Ley 2/2011, de 4 de marzo, de Economía Sostenible (en adelante LES), en su Disposición final Quincuagésima Sexta, introduce importantes modificaciones en el Título C.C.C. de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD).

En relación con dicha reforma, procede indicar que la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común –que, al decir de su Exposición de Motivos (punto 14) recoge "los principios básicos a que debe someterse el ejercicio de la potestad sancionadora de la Administración y los correspondientes derechos que de tales principios se derivan para los ciudadanos extraídos del Texto Constitucional y de la ya consolidada jurisprudencia sobre la materia"- sanciona el principio de aplicación retroactiva de la norma más favorable estableciendo en el artículo 128.2 que "las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor".

Por ello, deberá analizarse si el régimen sancionador derivado de la reforma operada en la LOPD por la LES, que entró en vigor al día siguiente de su publicación en el B.O.E., resulta más beneficioso para la presunta infractora en el presente procedimiento.

Por lo que aquí interesa, la LES ha modificado el intervalo de las cuantías de las sanciones correspondientes a las infracciones graves, imputadas en este caso, en el sentido de reducir el límite máximo y mínimo en estas infracciones. Por tanto, resulta aplicable al presente procedimiento la modificación introducida por la LES, debiendo aplicarse esta norma.

A lo anterior ha de añadirse que la LES ha añadido un nuevo apartado 6 al artículo 45 de la LOPD del siguiente tenor:

"Excepcionalmente el órgano sancionador podrá, previa audiencia de los

interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

Sin embargo la nueva redacción del artículo 45.4 de la LOPD incluye nuevos elementos, entre los que deben destacarse los siguientes:

- El volumen de negocio y actividad del infractor

- La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal

Del análisis de la concurrencia de los citados nuevos criterios se concluye, que en un caso como el presente, de empresas de destacado volumen de negocio con una actividad estrechamente relacionada con el tratamiento de datos personales, no procede la aplicación de la previsión contenida en el nuevo apartado 6 del artículo 45 LOPD, que permite apercibir al sujeto responsable en lugar de acordar la apertura de un procedimiento sancionador.

VIII

El artículo 45 .2 .3 .4 y .5 de la LOPD establece lo siguiente:

2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.
3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción

consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.»

La Sentencia de 21/01/2004 de la Audiencia Nacional, en su recurso 1939/2001, señaló que dicho precepto <<…no es sino manifestación del llamado principio de proporcionalidad (artículo 131.1 de la LRJPAC), incluido en el más general de prohibición de exceso, reconocido por la jurisprudencia como principio general del Derecho. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas, atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos.

Aplicando la anterior doctrina, la Audiencia Nacional exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o la cesión a terceros. Y ello porque siendo el de la protección de datos un derecho fundamental (Sentencia del Tribunal Constitucional 292/2000), los depositarios de estos datos deben ser especialmente diligentes y cuidadosos a la hora de operar con ellos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma. En este sentido, entre otras, Sentencias de la Audiencia Nacional de fechas 14 de febrero de 2002, 20 de septiembre de 2002, 13 de abril de 2005 y 18 de mayo de 2005.

El INSTITUTO CLINICO DE ALTA TECNOLOGIA, SA ha manifestado, en las alegaciones al acuerdo de inicio, que ni ICAT ni ninguno de los otros centros que operan bajo la marca "Creu Blanca", han recibido denuncia ni han sido sancionadas en materia de protección de datos. Por otra parte expresa que: "nos hemos puesto en contacto con nuestros informáticos para que cambien el diseño de la aplicación a los efectos de que, por más trato preferente que tengamos, en todo caso SIEMPRE Y TODO EL MUNDO, SIN EXCEPCION ALGUNA, habrá de firmar a partir de ahora el consentimiento por "escrito".

Es evidente que, a pesar de lo alegado, el INSTITUTO CLINICO DE ALTA TECNOLOGIA, SA no ha prestado la diligencia debida al vulnerar el principio del consentimiento para el tratamiento de los datos personales relativos a la salud del denunciante. No obstante, constatada la comisión de la infracción imputada, se aprecia en este caso la concurrencia del supuesto contemplado en el punto b del apartado 5 del artículo 45 de la LOPD dado que la entidad infractora manifiesta haber regularizado la situación irregular de forma diligente.

Concurren por tanto circunstancias que permiten apreciar una cualificada disminución de la culpabilidad imputada respecto de la comisión de dicha infracción, por lo que se estima que procede la aplicación del artículo 45.5 de la LOPD respecto de la misma, y establecer la cuantía de la sanción en la escala de las infracciones graves, no apreciándose obstáculo alguno ni indefensión o perjuicio para ninguna de las partes por dicha aplicación.

Por otra parte, respecto a los criterios de graduación de las sanciones recogidos en el artículo 45.4 de la LOPD, no se pueden ignorar circunstancias tales como la ausencia de beneficio, de intencionalidad y que es el primer expediente por hechos de esta naturaleza. Por todo ello, se estima ponderada y proporcionada a la gravedad del hecho la imposición al INSTITUTO CLINICO DE ALTA TECNOLOGIA, SA de una multa de 40.001 € (cuarenta mil un euros) por la vulneración del principio del consentimiento para el tratamiento de los datos personales relativos a la salud, recogido en el artículo 7.3 de la LOPD.

Con relación a lo alegado a este respecto por la MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA cabe destacar el hecho de que no se ha visto afectada por incumplimiento alguno de la LOPD. Sin embargo, conforme al criterio de la Audiencia Nacional sobre la diligencia exigible a las entidades que operan con datos personales, es evidente que, a pesar de lo alegado, MGC no ha prestado la diligencia debida al vulnerar el principio de seguridad de los datos personales relativos a la salud de sus trabajadores, que ha tenido como consecuencia que esos datos personales fueran accesibles por terceros no autorizados.

Respecto a los criterios de graduación de las sanciones recogidos en el artículo 45.4 de la LOPD es necesario tener en cuenta la entidad de la infracción cometida al vulnerar el principio de seguridad de los datos. Como ya se mencionó, el derecho fundamental a la protección de los datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona es decir, el poder de resguardar su vida privada de una publicidad no querida.

Por otra parte, a este respecto, tampoco pueden ignorarse las circunstancias de ausencia de beneficio, de intencionalidad y que es el primer expediente por incumplimiento de la LOPD. Por todo ello, se estima ponderada y proporcionada a la gravedad del hecho la imposición de una multa de 40.001 € (cuarenta mil un euros) por la vulneración del principio de seguridad de los datos que incumbe al responsable del fichero, recogido en el artículo 9 de la LOPD.>>

III

Insiste la recurrente en el argumento de que no se ha aportado prueba de pérdida, extravío, tratamiento o acceso no autorizado conforme a la infracción de resultado que, según su parecer, califica la Audiencia Nacional a la contenida en el artículo 9 de la LOPD. En apoyo de esta alegación presenta la recurrente varios antecedentes de esta Agencia con resultado de archivo porque no se produce el hecho protegido: la alteración, la pérdida, el tratamiento o el acceso no autorizado que es preciso para que se produzca la infracción prevista en el artículo 9 que, según su consideración, exige una obligación de resultado. Se hace una exposición conjunta de la vulneración del deber de guardar secreto y de la insuficiencia de medidas de seguridad: "*Dicha Sentencia declara algo que resulta evidente y es que la vulneración de la obligación de secreto exige revelar la información confidencial a un tercero.*
La Audiencia Nacional, como hemos señalado y probado anteriormente, ha calificado reiteradamente (Sentencias de 28 de junio de 2006, 11 de diciembre de 2008 y 25 de febrero de 2010) la obligación contenida en el artículo 9.1 de la LOPD como una obligación de resultado, compartiendo la misma naturaleza obligacional del artículo 10 de la LOPD.

La diferencia entre ambas obligaciones es que mientras el deber de secreto implica que la información no sea revelada a terceros, la obligación de adoptar medidas de seguridad implica que estas hayan sido adoptadas y se revelen eficaces, eficacia que se presumirá mientras no se pruebe la pérdida, extravío, tratamiento o acceso no autorizado."

Respecto de este argumento, como ya se expuso en la resolución recurrida, la Audiencia Nacional en la sentencia correspondiente al recurso 471/2008 expuso expresamente esta cuestión razonando "*La infracción tipificada en el art. 44.3 .g) es una infracción de resultado que exige que los datos personales sobre los que exista un deber de secreto profesional -como aquí ocurre en relación con el número de la cuenta corriente- se hayan puesto de manifiesto a un tercero, sin que pueda presumirse que tal revelación se ha producido. Efectivamente, la Agencia Española de Protección de Datos en su resolución se limita a poner de manifiesto que el sistema de cierre, mediante ventanilla transparente, de los sobres utilizados por el Banco para realizar determinadas comunicaciones a sus clientes pudiera dar lugar a que determinados datos personales contenidos en esas comunicaciones puedan ser conocidas por terceras personas respecto de las que deba mantenerse el secreto. No prueba sin embargo que los datos fueran efectivamente conocidos por dichos terceros. Estaríamos, por tanto, como sostiene el recurrente, ante una posible infracción de medidas de seguridad -que es una infracción de actividad- pero no ante la infracción que se le imputa que exige la puesta en conocimiento de un tercero de los datos personales.*"

De manera que puede decirse que lo argumentado por la entidad ahora recurrente, no es válido toda vez que se imputa la infracción prevista en el artículo 9 que es una infracción de actividad que no exige, como expresa la Audiencia Nacional, la puesta en conocimiento de un tercero de los datos personales, infracción ésta recogida en el artículo 10 de la LOPD como ya se expuso en la resolución ahora recurrida.

En este procedimiento se acreditó, por medio de la inspección llevada a cabo por esta Agencia, que los datos personales relativos a la salud de los trabajadores de la Mutua denunciada y en particular los del afectado en el procedimiento, se custodiaban en la caja acorazada de la entidad a la que sólo tenían acceso el Director General y el Director General Adjunto.

En las alegaciones al acuerdo de inicio del procedimiento sancionador ahora recurrido se manifestó que el acceso a la cámara acorazada estaba limitado, además de al Director Médico, al Director General y a los dos Directores Generales Adjuntos.

En escrito posterior se aclaró lo relativo a los accesos a los datos en cuestión, diciendo que, de las personas que tienen acceso a la caja donde se guardan los informes médicos de los empleados, solo las que forman parte del servicio médico de la entidad están autorizadas para acceder a ellos.

En el procedimiento ahora recurrido se acreditó por medio de inspección en la sede de la entidad, que los datos personales de los trabajadores de la recurrente eran accesibles por terceros no autorizados, personas que no pertenecen al servicio médico de la entidad, lo que establece la base de facto para fundamentar la imputación de la infracción del artículo 9.1 de la LOPD infracción calificada "*de actividad*", que no exige que se pruebe el efectivo conocimiento de los datos personales por un tercero.

Por otra parte cabe también recordar en este momento que la Audiencia Nacional, en sus sentencias de 13 de junio de 2002 y de 7 de febrero de 2003, entre otras, ha establecido que: "*No basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva ...*".

Por lo tanto, en el presente recurso de reposición, MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 26 de septiembre de 2011, en el procedimiento sancionador PS/00157/2011.

SEGUNDO: NOTIFICAR la presente resolución a la entidad MUTUA GENERAL DE CATALUNYA DE SEGUROS Y REASEGUROS A PRIMA FIJA.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto según lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta del referido texto legal.

Madrid, 25 de noviembre de 2011

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Rodríguez Álvarez