N/REF: 036833/2019

La consulta parte de lo señalado por esta Agencia en su Informe 11/2019 (N/Ref. 2995/2019), y solicita conocer el criterio de este Gabinete Jurídico sobre si es obligatoria la designación de más de un delegado de protección de datos en el ámbito del Ministerio de Defensa, teniendo en cuenta la existencia, dentro de su estructura, de diferentes centros docentes y sanitarios, a los que se referiría el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, considerando el solicitante que podría ser suficiente la designación de un delegado de protección de datos específico en el ámbito de la Inspección General de Sanidad, con competencia en los dos hospitales militares, en las diez unidades de reconocimiento pericial y en el Instituto de Medicina Preventiva de la Defensa, además del actual que seguiría teniendo competencias en el resto del ámbito del Ministerio de Defensa.

I

Como ha señalado reiteradamente esta Agencia y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”.

Un papel fundamental dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el delegado de protección de datos (DPD), que el Reglamento General regula en sus artículos 37 a 39. En particular, el artículo 37.1 a) impone obligatoriamente la designación de un delegado en los supuestos en que “el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial”, circunstancia que concurre en el Ministerio de Defensa.

No obstante, el artículo 37.1 del RGPD también contempla otros supuestos en los que deberá procederse al nombramiento de un DPD,

atendiendo al tipo de actividades que lleve a cabo el responsable (o encargado):

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Dicho precepto se complementa con lo dispuesto en el artículo 34.1 de la LOPDGDD, que especifica determinados supuestos en los que resulta obligatoria la designación de un DPD, entre los que se encuentra, tal y como se señala en la consulta, “los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas” y “los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes”.

Por consiguiente, la obligatoriedad en la designación de un DPD puede derivar de la naturaleza pública del responsable o de las características de las actividades de tratamiento, presentando, el presente caso, la singularidad de concurrir ambas circunstancias en la entidad consultante, al tratarse de una Administración Pública que realiza actividades de tratamiento que, en sí mismo consideradas, requerirían la designación obligatoria de un DPD. Así ocurre, por ejemplo, en el caso de los hospitales integrados en la red sanitaria militar, cuya actividad principal es prestar atención sanitaria lo que requiere el tratamiento, a gran escala, de los datos relativos a la salud de sus pacientes recogidos en las historias clínicas, siendo obligatoria la designación de un DPD conforme al citado artículo 34.1 l) de la LOPDGDD, o en el de los diferentes centros docentes integrados en la estructura de las Fuerzas Armadas, a los que resultaría de aplicación el artículo 34.1 b) de la misma.

En este sentido, en el Informe 11/2019 citado en la consulta, se planteaba una cuestión similar, si bien no idéntica, a la que es objeto del presente informe, ya que se trataba de un supuesto en el que se había designado un único DPD para todos los órganos de una misma Administración Pública autonómica y en el mismo se concluía que “el artículo 34 de la LOPDDD establece el **nombramiento específico de DPD** en el supuesto de los colegios profesionales y sus consejos generales, de los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas, y de los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes”.

No obstante, tal y como se plantea en la consulta, la exigencia del nombramiento específico de DPD no debe interpretarse, sin más, como la necesidad de nombrar diferentes DPD, como tampoco puede entenderse, como se concluía en el citado informe, en la procedencia del nombramiento de un único DPD, tal y como se analiza a continuación.

II

Para la adecuada resolución de la cuestión planteada, debe partirse de las importantes funciones que el artículo 39.1 del RGPD asigna al DPD:

> 1.El delegado de protección de datos tendrá como mínimo las siguientes funciones:
>
> a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
> b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
> c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
> d) cooperar con la autoridad de control;
> e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

Se trata, por consiguiente, de funciones de asesoramiento y supervisión dirigidas a garantizar el adecuado cumplimiento de la normativa sobre protección de datos personales, señalando el artículo 39.2 que “El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento”. Asimismo, el artículo 38.1 establece claramente que “El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales”.

Además de las importantes funciones de asesoramiento que el DPD tiene asignadas, incluidos los supuestos en los que sea necesario realizar una evaluación de impacto por tratarse de tratamientos de alto riesgo, y precisando las funciones de supervisión, el artículo 36 de la LOPDGDD prevé que "El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias", que "En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica" y que "Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento".

Asimismo, en cuanto a las relaciones con esta Agencia, debe tenerse en cuenta que corresponde al DPD, conforme al artículo 39.1.d) del RGPD, cooperar con la autoridad de control, siendo destacable a estos efectos la regulación que el artículo 37 de la LOPDGDD realiza de la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos:

> 1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.
>
> En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.
>
> 2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.
>
> Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.
>
> 3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

Por otro lado, el artículo 39.1.e) del RGPD establece también como funciones del DPD "actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto". Precisamente, atendiendo al nuevo modelo establecido en el RGPD y a las funciones encomendadas al DPD en cuanto al asesoramiento al responsable y a la realización de consultas a la AEPD, es criterio reiterado de este Gabinete Jurídico que "si el responsable del tratamiento tiene dudas sobre la base jurídica que pueda determinar la licitud de un determinado tratamiento deberá consultar a su delegado de protección de datos en los supuestos en que, como el presente, su designación es obligatoria, quien deberá prestarle el asesoramiento preciso. Sólo en el caso de que el delegado de protección de datos tuviera dudas jurídicas sobre el asunto sometido a su consideración que no puedan resolverse con los criterios ya informados por la AEPD o por tratarse de cuestiones nuevas derivadas de la aplicación del nuevo régimen jurídico de protección de datos de carácter personal y que tengan un alcance general en el que resulte conveniente un informe que contribuya a la seguridad jurídica, podrá elevar dicho delegado consulta a este Gabinete Jurídico, acompañando a dicha consulta su propio informe en el que se analicen detallada y motivadamente las cuestiones objeto de consulta".

Para el adecuado cumplimiento de dichos cometidos, el RGPD exige unos requisitos de capacitación del DPD, y que al mismo se le dote de los recursos necesarios.

En cuanto a los requisitos de capacitación, el artículo 37.5 dispone que "El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39".

Por su parte, el artículo 35 de la LOPDGDD añade que "El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos".

El Grupo del Artículo 29, en las ya citadas Directrices sobre los delegados de protección de datos, destaca, en relación con los conocimientos y habilidades del DPD, los siguientes puntos:

Nivel de conocimientos

El nivel de conocimientos requerido no está definido estrictamente pero debe ser acorde con la sensibilidad, complejidad y cantidad de los datos que una organización trata. Por ejemplo, cuando la actividad de tratamiento de los datos es especialmente compleja o cuando implica una gran cantidad de datos sensibles, el DPD podría necesitar un nivel mayor de conocimientos y apoyo. Existe también una diferencia dependiendo de si la organización transfiere sistemáticamente datos personales fuera de la Unión Europea o si dichas transferencias son ocasionales. Así pues, el DPD debe elegirse con cuidado, teniendo debidamente en cuenta las cuestiones relativas a la protección de datos que surjan en la organización.

Cualidades profesionales

Aunque el artículo 37, apartado 5, no especifica las cualidades profesionales que se deben tener en cuenta a la hora de designar al DPD, un factor importante es que este tenga conocimientos sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD. Resulta también de utilidad que las autoridades de control promuevan una formación adecuada y periódica para los DPD.

El conocimiento del sector empresarial y de la organización del responsable del tratamiento es también útil. Asimismo, el DPD debe tener un buen conocimiento de las operaciones de tratamiento que se llevan a cabo, así como de los sistemas de información y de las necesidades de seguridad y protección de datos del responsable del tratamiento.

En el caso de una autoridad u organismo público, el DPD debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización.

Capacidad para desempeñar sus funciones

La capacidad del DPD para desempeñar sus funciones debe interpretarse tanto en referencia a sus cualidades personales y conocimientos como a su puesto dentro de la organización. Las cualidades personales deben incluir, por ejemplo, la integridad y un nivel elevado de ética profesional; la principal preocupación del DPD debe ser posibilitar el cumplimiento del RGPD. El DPD desempeña un papel fundamental en la promoción de una cultura de protección de datos dentro de la organización y contribuye a la aplicación de elementos esenciales del RGPD, como los principios relativos al tratamiento de datos, los derechos de los interesados, la protección de los datos desde el diseño y por defecto, el registro de las actividades de tratamiento, la

seguridad del tratamiento y la notificación y comunicación de las violaciones de la seguridad de los datos.

Por otro lado, la necesidad de dotar al DPD de los recursos necesarios para el desempeño de sus funciones se recoge como una obligación del responsable en el artículo 38.2 del RGPD: “El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados”.

A este respecto, en las Directrices del Grupo del 29 se indica lo siguiente:

El artículo 38, apartado 2, del RGPD prevé que la organización respalde a su DPD «facilitando los recursos necesarios para el desempeño de [sus] funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados». Deben tenerse en cuenta, en especial, los siguientes aspectos:

Apoyo activo a la labor del DPD por parte de la alta dirección (al nivel del consejo de administración).

Tiempo suficiente para que el DPD cumpla con sus funciones, lo cual es particularmente importante cuando se designa un DPD interno a tiempo parcial o cuando el DPD externo lleva a cabo la protección de datos de manera complementaria a otras obligaciones. De otro modo, el conflicto entre prioridades podría dar lugar al descuido de las obligaciones del DPD. Es primordial contar con tiempo suficiente para dedicárselo a las tareas de DPD. Es una práctica recomendable establecer un porcentaje de tiempo para la labor propia del DPD cuando no se lleve a cabo a tiempo completo. Es también práctica recomendable determinar el tiempo necesario para realizar la labor, el nivel de prioridad adecuado para las funciones del DPD y para que el DPD (o la organización) redacte un plan de trabajo.

Apoyo adecuado en cuanto a recursos financieros, infraestructura (locales, instalaciones, equipos) y personal, según se requiera.

Comunicación oficial de la designación del DPD a todo el personal para garantizar que su existencia y función se conozcan dentro de la organización.

Acceso necesario a otros servicios, como recursos humanos, departamento jurídico, TI, seguridad, etc., de modo que los DPD puedan recibir apoyo esencial, aportaciones e información de dichos servicios.

Formación continua. Debe darse a los DPD la oportunidad de mantenerse al día con respecto a los avances que se den en el ámbito de la protección de datos. El objetivo debe ser mejorar constantemente el nivel de conocimientos de los DPD y se les debe animar a participar en cursos de formación sobre protección de datos y otras formas de desarrollo profesional, como la participación en foros privados, talleres, etc.

En función del tamaño y estructura de la organización, puede ser necesario establecer un equipo de DPD (un DPD y su personal). En esos casos, deben delimitarse con claridad la estructura interna del equipo y las tareas y responsabilidades de cada uno de sus miembros. De manera similar, cuando la función del DPD la ejerza un proveedor de servicios externo, un grupo de personas que trabaje para dicha entidad podrá realizar de manera eficaz las funciones de DPD como equipo, bajo la responsabilidad de un contacto principal designado para el cliente. En general, cuanto más complejas o sensibles sean las operaciones de tratamiento, más recursos deberán destinarse al DPD. La función de protección de datos debe desempeñarse con eficacia y dotarse con los recursos suficientes para el tratamiento que se esté realizando.

III

Una vez analizada la transcendencia de las funciones que el RGPD asigna al DPD y los requisitos de capacitación y recursos de los que debe dotarse al mismo, procede analizar la cuestión planteada en la consulta y que se centra en la necesidad de nombrar más de un DPD en el ámbito del Ministerio de Defensa. Para ello, debe partirse de lo señalado en el artículo 37.3 del RGPD, según el cual “Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño”. Se trata, por consiguiente, de la misma regla prevista en el apartado anterior del precepto para las entidades privadas, al señalar que “Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento”.

Esta cuestión es objeto de análisis en las Directrices sobre los delegados de protección de datos del Grupo del Artículo 29, cuyo apartado 2.3. se refiere a la designación de un DPD único para varias organizaciones:

> 2.3. Designación de un DPD único para varias organizaciones.
>
> El artículo 37, apartado 2, permite a un grupo empresarial designar un único DPD, siempre que este «sea fácilmente accesible desde cada establecimiento». La noción de accesibilidad se refiere a las tareas del DPD como punto de contacto con respecto a los interesados y a la autoridad de control, pero también internamente dentro de la organización, teniendo en cuenta que una de esas tareas es «informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento».

Con el fin de garantizar que el DPD, ya sea interno o externo, sea accesible, es importante asegurarse de que sus datos de contacto están disponibles de conformidad con los requisitos del RGPD.

El DPD, con ayuda de un equipo si es necesario, debe estar en condiciones de comunicarse eficazmente con los interesados y cooperar con las correspondientes autoridades de control. Esto significa también que dicha comunicación debe tener lugar en el idioma o idiomas utilizados por las autoridades de control y los interesados afectados. La disponibilidad de un DPD (ya sea físicamente en las mismas instalaciones como empleado, ya sea en línea o mediante otros medios seguros de comunicación) es fundamental para garantizar que los interesados puedan contactar con el DPD.

De conformidad con el artículo 37, apartado 3, se podrá designar un único DPD para varias autoridades u organismos públicos, teniendo en cuenta su estructura organizativa y tamaño. Las mismas consideraciones se aplican con respecto a los recursos y las comunicaciones. Puesto que el DPD se encarga de una variedad de tareas, el responsable o el encargado del tratamiento deben garantizar que un único DPD, con la ayuda de un equipo si fuera necesario, pueda realizar dichas tareas eficazmente a pesar de haber sido designado por varias autoridades y organismos públicos.

Por consiguiente, lo esencial no es el número de DPD, ni siquiera que estos formen parte de la organización del responsable (el apartado 6 del artículo 37 prevé que “el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios”) **sino que lo relevante es que los mismos reúnan los requisitos de capacitación e independencia que les permitan desarrollar adecuadamente las funciones que el RGPD les asigna,** teniendo en cuenta que, como recuerda el Considerando 97 del RGPD, “El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o encargado”.

Por tanto, siendo la designación de DPD en una Administración Pública una cuestión eminentemente organizativa, en los términos que se indican en el citado Informe 11/2019, y siempre que quede adecuadamente garantizada su independencia, **lo relevante es que las funciones que se asignan al DPD se puedan realizar con eficacia, debiendo tenerse en cuenta, igualmente, el criterio de la disponibilidad, fundamental para garantizar que los interesados puedan fácilmente contactar con el DPD** (conforme al artículo 38.4 del RGPD, “los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al

tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento").

Por tanto, dichas funciones podrán desarrollarse eficazmente si se cumplen con los requisitos de capacitación al proceder a la designación del DPD y se le dota de los recursos necesarios, incluido, como señala el Grupo del Artículo 29 un equipo de DPD (un DPD y su personal), equipo que deberá ser proporcional al tamaño y estructura de la organización, así como a la sensibilidad, complejidad y cantidad de los datos que una organización trata, debiendo garantizarse la disponibilidad del DPD de modo que los interesados puedan contactar con él, así como comunicarse con las autoridades de protección de datos.

En este sentido, han sido muchos los departamentos ministeriales que se han dotado de un único DPD, creando la infraestructura de apoyo que se ha considerado oportuna para el adecuado desempeño de sus funciones.

Sin embargo, en otras ocasiones, atendiendo a la estructura del departamento y a los diferentes tratamientos de datos realizados, se ha optado por la designación de diferentes DPD y la creación de órganos para la adecuada coordinación en el ejercicio de sus funciones. Ejemplo de esta organización es el Ministerio del Interior, tal y como se refleja en la Orden INT/424/2019, de 10 de abril, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior y las directrices generales en materia de seguridad de la información para la difusión de resultados provisionales en procesos electorales, en la que se constituye el Grupo de Trabajo de los Delegados de Protección de Datos, compuesto por los Delegados de Protección de Datos nombrados en el Ministerio del Interior: DPD de la Dirección General de la Policía, DPD de la Dirección General de la Guardia Civil, DPD de la Secretaría General de Instituciones Penitenciarias, DPD de la Dirección General de Tráfico, DPD de la Secretaría de Estado de Seguridad y DPD del Ministerio, para el ámbito del Ministro, y de la Subsecretaría del Interior (excluida la Dirección General de Tráfico).

En el presente caso, tal y como indica en su informe el DPD del Ministerio de Defensa, la estructura del Ministerio de Defensa "garantizaría que un DPD único (dotado de la infraestructura y equipo suficiente), pueda realizar sus tareas eficazmente, con el correcto desarrollo de sus funciones y la seguridad jurídica en su interlocución con los afectados, responsables y autoridades de control, teniendo en cuenta, además, la organización establecida en la Instrucción 16/2017, de 31 de marzo, del Secretario de Estado de Defensa, por la que se aprueban las normas de seguridad de la información que contenga datos de carácter personal en el Ministerio de Defensa. En dichas normas se establece la estructura funcional necesaria para ello, siendo de aplicación a todos los órganos del Ministerio y sus organismos autónomos".

No obstante lo anterior, el propio informe recoge que, según ha informado la Inspección General de Sanidad “en el Ministerio de Defensa se encuentran legalmente obligados al mantenimiento de los historiales clínicos dos centros hospitalarios, en Madrid y en Zaragoza, y 10 unidades de reconocimiento pericial que estarían incluidas dentro del concepto: ”centros de reconocimiento médico (proveedores de asistencia sanitaria sin internamiento)” que prestan el apoyo técnico pericial y administrativo que requieran las Juntas Periciales para emitir sus dictámenes. Además, el Instituto de Medicina Preventiva de la Defensa custodia documentación clínica relacionada con el historial de vacunaciones del personal de las Fuerzas Armadas. Todos ellos con dependencia orgánica de la Inspección General de Sanidad”. De ahí que el DPD del Ministerio de Defensa plantee que “No obstante lo anterior, también es cierto que en razón de la naturaleza y alcance de las operaciones de tratamiento de categorías especiales de datos personales, que se llevan a cabo, fundamentalmente en los dos hospitales militares y en menor medida en el resto de centros sanitarios, pudieran aconsejar la existencia de un Delegado de Protección de Datos específico en el ámbito de los centros sanitarios, pero no uno específico para cada uno de ellos, sino un único DPD en el ámbito de la Inspección General de Sanidad de la Defensa, responsable en el ámbito del Ministerio de Defensa del tratamiento de dichos datos, dada la dependencia funcional y orgánica, así como las funciones que se le atribuyen a la misma, en el Real Decreto de estructura de este departamento”.

Esta Agencia comparte el criterio del Ministerio de Defensa, atendida la especial naturaleza de los datos que se tratan (datos de salud, incluidos dentro de las categorías especiales de datos conforme al artículo 9 del RGPD), del número de tratamientos y personas afectadas, especialmente en el caso de los hospitales militares, que prestan, en virtud de convenio, servicios de asistencia sanitaria especializada a los usuarios del Sistema Sanitario Público, del riesgo inherente a dichos tratamientos que requieren la realización de una evaluación de impacto, la normativa especial aplicable, como ocurre, por ejemplo, en materia de acceso a historias clínicas, el elevado número de reclamaciones que se plantean en este ámbito, etc.

Por lo tanto, se considera conveniente la designación de un DPD específico en este ámbito, correspondiendo al responsable valorar si es suficiente con un único DPD para todos los órganos integrados en la Inspección General de Sanidad o, especialmente en el caso de los hospitales, un DPD por centro, atendiendo a los requisitos de suficiencia de medios anteriormente expuesto.

En cuanto al mantenimiento de un único DPD con competencias en el resto del Ministerio de Defensa, incluidos los numerosos centros docentes militares que del mismo dependen, se trata de una decisión del responsable que esta Agencia considera admisible, siempre que se cumplan con los requisitos de capacitación, suficiencia de medios, disponibilidad e

independencia que establece el RGPD, y que se garantice que participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales. A estos efectos, resulta oportuno solicitar el asesoramiento del propio DPD, tal y como se ha hecho por el Ministerio de Defensa, siendo su criterio favorable a dicha posibilidad.

IV

Atendiendo a lo señalado en el presente informe, y ya al margen de lo solicitado en la presente consulta, **esta Agencia debe incidir, una vez más, en la importancia que la figura del DPD tiene en el nuevo modelo instaurado por el RGPD y que pivota sobre la base de la responsabilidad proactiva del responsable.** De acuerdo con el mismo, en los casos en que resulte obligatorio o así se haya estimado adecuado con carácter voluntario, **ha de ser el responsable el que valore la procedencia de designar uno o varios DPD, así como si el mismo ha de pertenecer o no a su propia estructura, garantizando en todo momento su independencia y disponibilidad.** Asimismo, **deberá garantizar que el DPD cumple con los requisitos de capacitación adecuados y que se le dota de los medios personales y materiales necesarios** para la realización eficaz de las funciones que tiene encomendadas, que **participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales** y que **rinde cuentas al más alto nivel jerárquico**, **documentando adecuadamente** el responsable, conforme al ya citado principio de responsabilidad proactiva, todas las decisiones que adopte a este respecto, para poder demostrarlo a requerimiento de las autoridades de control. **De este modo, quedará garantizado que el nombramiento del DPD no se ha realizado con carácter meramente formal y que el mismo cumple eficazmente con las funciones que le asigna el RGPD, siendo el primer interesado en dicha eficacia el propio responsable, que es quien responderá, y no el DPD, en caso de inobservancia del RGPD.**