Dictamen en relación con una consulta sobre la utilización del número de DNI para acceder a un sistema de información de un ayuntamiento

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito en el que se plantea si la utilización del número de DNI para acceder a un sistema de información de un ayuntamiento, a los efectos de tramitar la tarjeta bonificada a personas en situación de desempleo, se adecua a la legislación en materia de protección de datos de carácter personal.

Se adjunta al escrito de consulta copia del contrato de encargado del tratamiento suscrito entre la Autoritat del Transport Metropolità y el Institut Municipal de Serveis Socials del ayuntamiento.

Una vez analizada la petición y la documentación que la acompaña, y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente.

I

(...)

II

(...) manifiesta, en su escrito de consulta, que la Autoritat del Transport Metropolità (en adelante, ATM) acordó ampliar las personas que pueden ser beneficiarias de la tarjeta bonificada para personas en situación de desempleo a aquellas personas que, pese a no percibir ayuda alguna del Estado, reciban ayudas por parte de los servicios sociales de los ayuntamientos integrados dentro del ámbito de la ATM.

A continuación expone que, a los efectos de facilitar la gestión y la tramitación de esta tarjeta bonificada respecto las personas que reciben ayudas de los servicios sociales del ayuntamiento, se suscribió un contrato de encargado del tratamiento entre la ATM i el Institut Municipal de Serveis Socials (IMSS), del que se adjunta copia.

Asimismo informa que, en virtud de este contrato de encargado, el IMSS autoriza expresamente a la ATM a subencargar el tratamiento de los datos personales objeto del contrato a los operadores de transporte, entre los que se encuentra Transports Metropolitans de Barcelona (en adelante, TMB), puesto que el acceso a los datos por parte de los mismos se considera imprescindible para la implementación efectiva de la prestación y para la gestión de los correspondientes títulos de transportes y de sus beneficiarios.

Dicho esto, expone que el IMSS pone a disposición de los empleados de TMB la aplicación SIAS para poder consultar, en el marco del proceso de tramitación de la tarjeta bonificada, si la persona que la solicita puede ser beneficiaria o no de la misma. En concreto, señala que el acceso de los trabajadores a esta aplicación del IMSS se efectúa mediante la introducción del número de DNI:

(...) plantea a esta Autoridad las siguientes cuestiones:

a) Si los datos solicitantes para acceder al sistema SIAS (número de DNI de los agentes de información y atención ciudadana de TMB) son proporcionales en lo que

se refiere a su finalidad y, en consecuencia, si puede requerir al empleado el acceso al sistema como usuario a través de su DNIR y si esta exigencia es respetuosa con los principios que rigen en materia de protección de datos personales.

b) En todo caso, cuál se puede entender que es la base legal del tratamiento descrito (comunicación del número de DNI de ciertos empleados de TMB al ayuntamiento a través de la base de datos SIAS).

Estas cuestiones se examinan en los apartados siguientes de este dictamen.

Antes, informamos que, en atención al contrato de encargado del tratamiento aportado, las consideraciones efectuadas a lo largo de este dictamen son aplicables solamente con respecto al personal de TMB pero no se incluiría al personal que no ostente dicha condición.

III

El Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD), plenamente aplicable desde el pasado 25 de mayo (artículo 99), establece que todo tratamiento de datos personales tiene que ser lícito (artículo 5.1.a)) y, en este sentido, establece un sistema de legitimación del tratamiento de datos que se fundamenta en la necesidad de que concurra alguna de las bases jurídicas que establece el artículo 6, que no guardan entre si ni relación de prioridad ni de prelación.

El mencionado artículo 6.1 del RGPD en concreto dispone que:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

Por su parte, el artículo 6.3 del RGPD dispone que la base del tratamiento indicado en los apartados c) y e) de este artículo 6.1 del RGPD tiene que estar establecida por el Derecho de la Unión Europea o por el Derecho de los Estados Miembros que se aplique al responsable del tratamiento.

Pese a que el considerando 41 del RGPD dispone que *"cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento"*, hay que tener en cuenta

que el mismo considerando establece que ello *"sin perjuicio de los requisitos de conformidad con el ordenamiento constitucional del Estado miembro de que se trate"*.

La remisión a la base legítima establecida conforme al derecho interno de los Estados Miembros a la que se refiere el artículo 6.3 del RGPD requiere, en el caso del Estado Español, que la norma de desarrollo, por tratarse de un derecho fundamental, tenga rango de ley (artículo 53 CE).

En este sentido, el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Consejo de Ministros el 10 de noviembre de 2017 (BOCG, serie A, núm. 13-1, de 24.11.2017), aunque no resulta aplicable por motivos obvios, establece:

> *"Artículo 8. Tratamiento de datos amparado por la ley.*
> *1. El tratamiento de datos de carácter personal sólo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1 c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. La ley podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el Capítulo IV del Reglamento (UE) 2016/679.*
> *2. El tratamiento de datos de carácter personal sólo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por la ley".*

Así pues, para considerar que los tratamientos de datos están amparados por las bases jurídicas del artículo 6.1.c) y e) del RGPD debe existir una previsión normativa con rango de ley.

La Ley 12/2007, de 11 de octubre, de servicios sociales establece que:

> *"Artículo 27*
> *Responsabilidades públicas*
> *1. La Administración de la Generalitat, los municipios y los demás entes locales de Cataluña son las administraciones competentes en materia de servicios sociales, de acuerdo con lo establecido por el presente título y, si procede, la legislación sobre organización territorial y régimen local.*
> *2. Los municipios y los demás entes locales pueden ejercer competencias propias de la Administración de la Generalitat por vía de delegación, de encargo de gestión o de fórmulas de gestión conjunta, sin perjuicio de las competencias que las leyes les atribuyen".*

El artículo 31 de esta misma Ley a la que nos remitimos determina las competencias que corresponden a los municipios en materia de servicios sociales.

Por su parte, la Carta Municipal de Barcelona, aprobada por la Ley 22/1998, de 30 de diciembre, determina las competencias que, entre otras materias, le corresponden específicamente al municipio de Barcelona en materia de servicios sociales (Título VI, Capítol X).

El IMSS es el organismo autónomo creado por el ayuntamiento para impulsar, organizar y articular los servicios de atención social básica de responsabilidad municipal dirigidos a todas las personas que residen en esta ciudad.

A la vista de estas previsiones, se puede decir que, con carácter general, los tratamientos de datos personales efectuados por el IMSS en cumplimiento de las obligaciones establecidas en la Ley 12/2007 responden al ejercicio *"de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*", por lo que estarían legitimados por el artículo 6.1.e) del RGPD.

IV

Dicho esto, hay que tener presente que los tratamientos de estos datos por parte del IMSS deben adecuarse también al resto de principios establecidos en el RGPD, especialmente, a los efectos que interesan en el presente caso, al principio de integridad y confidencialidad.

El artículo 5 del RGPD establece que:

> *"1. Los datos personales serán:*
> *(...)*
> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".*

Sobre esto, el artículo 24 del RGPD dispone que:

> *"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*
> *(…)".*

Así pues, hay que tener en cuenta que el RGPD impone la obligación al responsable del tratamiento de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales que se tratarán. Cabe decir que es una obligación que también hace extensible al encargado del tratamiento (artículo 28.3.c) RGPD) y, si procede, al subencargado (artículo 28.4 RGPD).

En este punto, cabe señalar que el RGPD configura un sistema de seguridad que no se basa en los niveles de seguridad básico, medio y alto que preveía el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), sino en determinar, a partir de una valoración previa de los riesgos, qué medidas de seguridad son necesarias en cada caso (considerando 83 y artículo 32).

Por lo tanto, desde el pasado 25 de mayo, el esquema de medidas de seguridad previsto en el RLOPD no se puede considerar válido de manera automática. En algunos supuestos se podrán seguir aplicando estas mismas medidas si tras el análisis de riesgos previo se concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado para el caso concreto, pero en otros casos puede ser necesario completarlas con medidas adicionales.

Cabe indicar que, en el caso de las administraciones públicas, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de

Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero, que actualmente está siendo objeto de revisión.

En este sentido, el Proyecto de la LOPD citado anteriormente dispone que:

> *"Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.*
>
> *El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679".*

En cualquier caso, en atención a estos preceptos, está claro que corresponde al IMSS la implementación de estas medidas de seguridad con respecto a los tratamientos de datos de los que es responsable.

En el presente caso y por la información de que se dispone, el IMSS es responsable del sistema de información SIAS, que contiene los datos personales de las personas usuarias de los servicios sociales municipales.

Así pues, en materia de seguridad corresponde al IMSS, entre otras actuaciones, determinar qué personas deben acceder y tratar la información personal que contiene este sistema de información, así como adoptar mecanismos apropiados que permitan su correcta identificación y autenticación como usuarios del sistemas, a los efectos de garantizar, tal y como exige el RGPD, que no se produzcan tratamientos no autorizados. Todo ello con independencia de que se trate de su propio personal o bien de terceras personas ajenas al IMSS.

El cumplimiento de esta obligación que impone el RGPD puede justificar el tratamiento de determinados datos personales por parte del IMSS.

Según se desprende del contrato de encargado del tratamiento suscrito entre la ATM y el IMSS, adjunto al escrito de consulta, el IMSS ha autorizado que los trabajadores de TMB que tienen asignadas funciones de gestión y tramitación de la tarjeta bonificada para personas en situación de desempleo puedan acceder a sus sistema de información SIAS para poder consultar, en el marco del procedimiento de expedición, si la persona que solicita la tarjeta puede o no ser beneficiaria de la misma (acuerdo 1º). La información a la que podrán acceder estos trabajadores comprende la verificación (positiva o negativa) del cumplimiento de los requisitos exigidos para poder adquirir la tarjeta bonificada. TMB actuaría, con respecto al tratamiento de estos datos, como subencargado del tratamiento (acuerdo 4º).

De acuerdo con las manifestaciones efectuadas en el escrito de consulta, este acceso al sistema SIAS por parte del personal autorizado de TMB (agentes de información y atención ciudadana) se produce a través de la introducción de su número de DNI.

No está claro si, de toda la información facilitada, este dato es el único que se utiliza para acceder al sistema SIAS. De ser el caso, cabe decir que la identificación solamente a través de un usuario no parece lo bastante segura puesto que no garantiza la autenticación, es decir, no permite tener la certeza de que la persona que intenta acceder al sistema de información realmente sea quien dice ser. Pero especialmente resulta poco fiable si el usuario otorgado coincide con el número de DNI.

Con carácter general, hay que reconocer que, aunque el número de DNI no es un número de identificación destinado a ser de público conocimiento, lamentablemente a menudo aparece publicado, en ocasiones sin base legal, en instrumentos de distinta naturaleza (diarios oficiales, webs, etc.). Si bien esta Autoridad ha advertido en numerosas ocasiones de los efectos perniciosos de esta práctica, lo cierto es que hoy día aun hay muchos números de DNI que resultan fácilmente accesibles. Por lo tanto, emplear el número de DNI como único identificador para poder acceder a un sistema de información al que solamente determinadas personas deberían tener capacidad de acceso no resultaría una medida de seguridad adecuada.

Una cuestión diferente es que se utilice este dato relativo al número de DNI para identificarse como usuario del sistema SIAS y se combine esta información con un sistema de autenticación basado en la existencia de contraseñas.

Este tipo de mecanismo de identificación y autenticación (usuario y contraseña) es el método más extendido para impedir accesos no autorizados en sistemas o contenidos dentro de un sistema de información. Se trata de una medida establecida en estándares internacionales y en certificaciones en materia de seguridad informática (como la Norma ISO/IEC 27001 sobre la gestión de la seguridad de la información) y también reconocida por nuestro ordenamiento jurídico.

Así, por ejemplo, la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPACAP), dispone que:

> *"Artículo 9. Sistemas de identificación de los interesados en el procedimiento.*
> *1. Las Administraciones Públicas **están obligadas a verificar la identidad** de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el **Documento Nacional de Identidad** o documento identificativo equivalente.*
> *2. Los interesados **podrán identificarse electrónicamente** ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad. En particular, serán admitidos, los sistemas siguientes:*
> *a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.*
> *b) Sistemas basados en certificados electrónicos reconocidos o cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».*
> *c) Sistemas de clave concertada y **cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan**.*
> *(…)".*

Por su parte, el artículo 93 del RLOPD (aplicable en lo que no se oponga al RGPD) también disponía que el responsable tenía que establecer un mecanismo que permitiera la identificación inequívoca de cualquier usuario que intentara acceder a un sistema de información y también verificar que estuviera autorizado. En este sentido, admitía el uso de mecanismos de autenticación basados en la existencia de contraseñas.

Así pues, se pude decir que, con carácter general, la utilización de un usuario y de una contraseña como mecanismo de identificación y autenticación para acceder a un determinado sistema de información se considera una medida de seguridad adecuada. Sin

perjuicio de que, en atención al riesgo que conlleve el tratamiento de la información de que se trate, pueda resultar necesario establecer otros tipos de mecanismos más robustos (por ejemplo, basados en certificados electrónicos, etc.).

V

Partiendo de la premisa de que en el presente caso el acceso al sistema de información SIAS para los trabajadores de (...) que tienen encomendada la tramitación y expedición de la tarjeta bonificada para personas en situación de desempleo se efectúa a través de un mecanismo de identificación y autenticación basados en un usuario y una contraseña, hay que examinar específicamente si el uso del dato relativo al número de DNI como usuario resulta adecuado desde el punto de vista de la protección de datos.

El artículo 5 del RGPD, que ya hemos citado, dispone que:

"1. Los datos personales serán:
(...)
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
(...)".

Desde el punto de vista de la gestión de los sistemas de información, el nombre de usuario responde a la pregunta "¿quién eres?". Si tenemos en cuenta esto y la necesidad de garantizar que no se produzcan accesos no autorizados, está claro que tiene que reunir una característica fundamental: tiene que ser único.

En este sentido, y en atención al contexto en el que nos encontramos (acceso a la información personal en el marco de un procedimiento administrativo) el nombre y apellidos (identificación directa) o un número de identificación personal (identificación indirecta) probablemente serían los datos personales más adecuados.

En función de la dimensión y la estructura de la organización, o de su naturaleza, la gestión de los nombres de usuario puede ser un proceso laborioso. Así, por ejemplo, la utilización del nombre propio de la persona autorizada para acceder al sistema como nombre de usuario puede ser una opción viable en un ente pequeño, pero no así en un organismo de dimensiones medianas o grandes. En organizaciones con estructuras bien definidas puede resultar de utilidad añadir un código, por ejemplo del departamento, como parte del nombre de usuario. En otras ocasiones, las características propias del trabajo que lleva a cabo el personal autorizado puede requerir preservar su identidad, por ejemplo, por motivos de seguridad personal; por lo tanto, en estos casos, la utilización de un número de identificación personal específico podría ser preferible. En otros, también hay que autorizar accesos a personal ajeno al de la propia organización. Sea como fuere, una correcta gestión de las cuentas de usuarios obliga, en cualquier caso, a velar por que los nombres de usuarios empleados no coincidan para evitar así el riesgo de un acceso por parte de personas no autorizadas o a información personal indebida.

El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y de sus certificados de firma electrónica, dispone que:

"Artículo 1. Naturaleza y funciones.
*1. **El Documento Nacional de Identidad es un documento personal e intransferible** emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.*

2. Dicho Documento ***tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen****, así como la nacionalidad española del mismo.*
3. ***A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general****.*
4. ***Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular****, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.*
En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.
5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
6. Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento".

Como el DNI es el documento creado expresamente para acreditar inequívocamente la identidad de la persona que lo posee, podría decirse que se erige como un mecanismo óptimo en términos de identificación de usuarios.

Prueba de ello es que el legislador lo ha escogido como mecanismo de identificación electrónica de los ciudadanos que en todo caso tendrá que ser admitido por las administraciones públicas cuando estos se relacionan con ellas por medios electrónicos.

También hay que tener presente que la LPACAP establece en el artículo 9.1, ya citado, que el DNI es el documento a través del que las administraciones públicas han de verificar la identidad de las persones interesadas en el procedimiento administrativo.

Así pues, aunque no es imprescindible que el nombre de usuario de un sistema de información coincida con el número de DNI de la persona autorizada para acceder al mismo, no se puede decir que, desde el punto de vista de la protección de datos, resulte un dato personal inadecuado o no pertinente, puesto que su utilización ciertamente permite alcanzar el fin para el que se trata en el presente caso, a saber: garantizar de manera inequívoca la identidad de la persona usuaria del sistema de información.

Por lo tanto, con carácter general, se puede decir que su tratamiento se adecuaría al principio de minimización de datos (artículo 5.1.c) RGPD).

VI

En el escrito de consulta, también se plantea cuál es la base legal que legitimaría la comunicación del dato relativo al número de DNI de los trabajadores de TMB al IMSS.

Como se ha visto, el RGPD obliga a (...) a adoptar las medidas técnicas necesarias para evitar tratamientos no autorizados (artículos 5.1.f), 24 y 32), por lo tanto, a velar por que solamente las personas legitimadas puedan tener acceso a su sistema SIAS y únicamente a los datos personales que, en cada caso, resulten estrictamente necesarios (artículo 5.1.c) RGPD).

En el presente caso, existe un contrato de encargado del tratamiento entre el IMSS y la ATM suscrito para establecer un mecanismo de colaboración y cooperación entre ambas entidades para facilitar la tramitación de la tarjeta bonificada para aquellas personas residentes en el municipio que, al recibir algún tipo de ayuda de los servicios sociales del ayuntamiento, podrían ser beneficiarias de la misma.

El desarrollo y la ejecución de este encargo implican que los distintos operadores del transporte público tienen que poder consultar determinada información personal en poder del IMSS. Por este motivo, el IMSS autoriza expresamente a la AMT a subencargar el tratamiento de los datos personales vinculados o relacionados con la tramitación de este título de transporte bonificado a dichos operadores, entre otros, TMB.

En virtud de este subencargo del tratamiento (artículo 28.4 RGPD), el personal de (...) que tenga expresamente asignadas funciones de tramitación de los distintos títulos de transporte integrado estará legitimado para acceder al sistema SIAS.

Para hacer efectivo este acceso (para establecer los correspondientes permisos de acceso al SIAS), el IMSS requiere que TMB le comunique por adelantado cuáles son estas personas (según la información aportada, los agentes de información y atención ciudadana).

Por lo tanto, en la medida en que la comunicación del número de DNI de los trabajadores de TMB al IMSS sería con el fin de identificar a aquellas personas de su personal que, en atención a las funciones que tienen asignadas en virtud de su contrato laboral (artículo 20 del ET), tienen que poder acceder al sistema SIAS para poder gestionar de manera efectiva la tramitación de la tarjeta bonificada, el tratamiento de este dato (la comunicación del número de DNI) se podría considerar amparado en el marco de ejecución de un contrato, en base a lo dispuesto en el artículo 6.1.b) del RGPD.

Dicho esto, se hace notar que el contrato de encargo del tratamiento suscrito entre el IMSS y la ATM debería ser objeto de revisión a los efectos de adecuarlo a las previsiones del artículo 28.3 del RGPD. En este sentido, podría ser de interés consultar la Guía sobre el encargado del tratamiento en el RGPD, elaborada por las autoridades de protección de datos para ayudar a los responsables y encargados a adaptarse a las exigencias del RGPD, disponible en el web de la Autoridad http://apdcat.gencat.cat/ca/inici/.

De acuerdo con las consideraciones hechas hasta aquí en relación con la consulta planteada, se llega a las siguientes

Conclusiones

El establecimiento por parte del IMSS de un mecanismo de identificación y autenticación basado en el uso de un usuario que consiste en el número de DNI y de una contraseña para aquellos trabajadores de TMB que, en virtud de su condición de personal de un subencargado del tratamiento, tienen que poder acceder al sistema SIAS para ejercer las funciones que tienen encomendadas (tramitación de la tarjeta bonificada para las personas en situación de desempleo) podría considerarse una medida de seguridad adecuada, con base jurídica en el artículo 6.1.b) del RGPD, al ser necesario para la ejecución del contrato.

Barcelona, 18 de julio de 2018