Dictamen en relació amb una consulta sobre la utilització del número de DNI per accedir a un sistema d'informació d'un ajuntament

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit en què es planteja si la utilització del número de DNI per accedir a un sistema d'informació d'un Ajuntament, als efectes de tramitar la targeta bonificada per a persones en situació d'atur, s'adequa a la legislació en matèria de protecció de dades de caràcter personal.

S'adjunta, a l'escrit de consulta, còpia del contracte d'encarregat del tractament subscrit entre l'Autoritat del Transport Metropolità i l'Institut Municipal de Serveis Socials de l'Ajuntament.

Analitzada la petició i la documentació que l'acompanya, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

(...) manifesta, en el seu escrit de consulta, que l'Autoritat del Transport Metropolità (en endavant, ATM) va acordar ampliar les persones que poden ésser beneficiàries de la targeta bonificada per a persones en situació d'atur a aquelles persones que, tot i no percebre cap ajuda per part de l'Estat, rebessin ajudes per part dels serveis socials dels ajuntaments integrats dins l'àmbit de l'ATM.

Tot seguit exposa que, als efectes de facilitar la gestió i la tramitació d'aquesta targeta bonificada respecte les persones que reben ajuts dels serveis socials de l'Ajuntament, es va subscriure un contracte d'encarregat del tractament entre l'ATM i l'Institut Municipal de Serveis Socials (IMSS), del qual s'adjunta còpia.

Fa avinent, així mateix, que, en virtut d'aquest contracte d'encarregat, l'IMSS autoritza expressament a l'ATM a subencarregar el tractament de les dades personals objecte del contracte als operadors de transport -entre els quals es troba Transports Metropolitans de Barcelona (en endavant, TMB)-, atès que l'accés a les dades per aquests es considera imprescindible per a l'efectiva implementació de la prestació i per a la gestió dels corresponents títols de transports i dels seus beneficiaris.

Dit això, exposa que l'IMSS posa a disposició dels empleats de TMB l'aplicació SIAS, per, en el si del procés de tramitació de la targeta bonificada, poder consultar si la persona que la sol·licita en pot ser o no beneficiària. Particularment, assenyala que l'accés dels treballadors a aquesta aplicació de l'IMSS s'efectua mitjançant la introducció del número del DNI.

(...) planteja a aquest Autoritat les qüestions següents:

a) Si les dades sol·licitades per accedir al sistema SIAS (número de DNI dels agents d'informació i atenció ciutadana de TMB) són proporcionals pel que fa a la seva finalitat i, en conseqüència, si pot requerir a l'empleat el seu accés al sistema com a

usuari a través del seu DNI i si aquesta exigència és respectuosa amb els principis que regeixen en matèria de protecció de dades personals.

b) En tot cas, quina es pot entendre que és la base legal del tractament descrit (comunicació del número de DNI de certs empleats de TMB a l'Ajuntament a través de la base de dades SIAS).

Aquestes qüestions s'examinen en els apartats següents d'aquest dictamen.

Abans, fer avinent que, en atenció al contracte d'encarregat del tractament aportat, les consideracions efectuades al llarg d'aquest dictamen són aplicables només respecte el personal de TMB però no abastaria altre personal que no ostenti aquesta condició.

III

El Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (en endavant, RGPD), plenament aplicable des del darrer 25 de maig (article 99), estableix que tot tractament de dades personals ha de ser lícit (article 5.1.a)) i, en aquest sentit, estableix un sistema de legitimació del tractament de dades que es fonamenta en la necessitat de que concorri alguna de les bases jurídiques establertes al seu article 6, les quals no mantenen entre sí cap relació de prioritat o prelació.

L'esmentat article 6.1 de l'RGPD disposa, en concret, 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."

Per la seva part, l'article 6.3 de l'RGPD disposa que la base del tractament indicat als apartats c) i e) d'aquest article 6.1 de l'RGPD ha d'estar establerta pel Dret de la Unió Europea o pel dret dels Estats membres que s'apliqui al responsable del tractament.

Malgrat que el considerant 41 de l'RGPD disposa 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"*, cal tenir en compte que el mateix considerant estableix que això *"sin perjuicio de los requisitos de conformidad con el ordenamiento constitucional del Estado miembro de que se trate"*.

La remissió a la base legítima establerta conforme el dret intern dels estats membres a què fa referència l'article 6.3 de l'RGPD requereix, en el cas de l'Estat Espanyol, que la norma de desenvolupament, per tractar-se d'un dret fonamental, tingui rang de llei (article 53 CE).

En aquest sentit, el Projecte de Llei Orgànica de Protecció de Dades de Caràcter Personal, aprovat pel Consell de Ministres el 10 de novembre de 2017 (BOCG, sèrie A, núm. 13-1, de 24.11.2017), encara que per raons òbvies no resulta aplicable, estableix:

> *"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."*

Així doncs, per considerar els tractaments de dades emparats per les bases jurídiques de l'article 6.1.c) i e) de l'RGPD ha d'existir una previsió normativa amb rang de llei.

La Llei 12/2007, d'11 d'octubre, de serveis socials, estableix que:

> *"Article 27*
> *Responsabilitats públiques*
> *1. L'Administració de la Generalitat, els municipis i els altres ens locals de Catalunya són les administracions competents en matèria de serveis socials, d'acord amb el que estableix aquest títol i, si escau, la legislació sobre organització territorial i règim local.*
> *2. Els municipis i els altres ens locals poden exercir competències pròpies de l'Administració de la Generalitat per via de delegació, d'encàrrec de gestió o de fórmules de gestió conjunta, sens perjudici de les competències que les lleis els atribueixen."*

L'article 31 d'aquesta mateixa Llei, a què es remetem, determina les competències que corresponen als municipis en matèria de serveis socials.

Per la seva part, la Carta municipal de Barcelona, aprovada per la Llei 22/1998, de 30 de desembre, determina les competències que, entre d'altres matèries, li corresponen específicament al municipi de Barcelona en matèria de serveis socials (Títol VI, Capítol X).

L'IMSS és l'organisme autònom creat per l'Ajuntament per impulsar, organitzar i articular els serveis d'atenció social bàsica de responsabilitat municipal adreçats a totes les persones que resideixen en aquesta ciutat.

A la vista d'aquestes previsions, pot dir-se que, amb caràcter general, els tractaments de dades personals efectuats per l'IMSS en compliment de les obligacions establertes a la Llei 12/2007 responen a l'exercici *"de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*", per la qual cosa estarien legitimats per l'article 6.1.e) de l'RGPD.

IV

Dit això, cal tenir present que els tractaments d'aquestes dades per l'IMSS han d'adequar-se també a la resta de principis establerts a l'RGPD, especialment, als efectes que interessen en el present cas, al principi d'integritat i confidencialitat.

L'article 5 de l'RGPD estableix 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 això, l'article 24 de l'RGPD disposa 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.*
> *(…)".*

Cal tenir en compte, per tant, que l'RGPD imposa l'obligació al responsable del tractament d'adoptar les mesures tècniques i organitzatives necessàries per garantir la seguretat de les dades personals que seran tractades. Obligació que, cal dir, també fa extensible a l'encarregat del tractament (article 28.3.c) RGPD) i, si escau, subencarregat (article 28.4 RGPD).

Assenyalar, en aquest punt, que l'RGPD configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt que es preveien al Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD), sinó en determinar, arran d'una prèvia valoració dels riscos, quines mesures de seguretat són necessàries en cada cas (Considerant 83 i article 32).

Per tant, l'esquema de mesures de seguretat previst a l'RLOPD no pot, des del darrer 25 de maig, considerar-se vàlid de manera automàtica. En alguns supòsits es podran seguir aplicant aquestes mateixes mesures si de l'anàlisi de riscos previ es conclou que les mesures són realment les més adequades per oferir un nivell de seguretat adequat al cas concret, però en d'altres pot ser necessari completar-les amb mesures addicionals.

Fer també avinent que, en el cas de les administracions públiques, l'aplicació de les mesures de seguretat estarà marcada pels criteris establerts a l'Esquema Nacional de Seguretat, aprovat pel Reial Decret 3/2010, de 8 de gener, que, actualment, està sent objecte de revisió.

En aquest sentit, el Projecte de l'LOPD, abans citat, disposa 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 qualsevol cas, en atenció a aquests preceptes, és clar que correspon a l'IMSS la implementació d'aquestes mesures de seguretat respecte els tractaments de dades de què és responsable.

En el present cas i per la informació de què es disposa, l'IMSS és responsable del sistema d'informació SIAS, en què es contenen les dades personals de les persones usuàries dels serveis socials municipals.

Correspon, per tant, a l'IMSS, entre d'altres actuacions en matèria de seguretat, determinar quines persones han d'accedir i tractar la informació personal continguda en aquest sistema d'informació, així com adoptar mecanismes apropiats que permetin la seva correcta identificació i autenticació com a usuaris del sistema, als efectes de garantir, tal com exigeix l'RGPD, que no es produiran tractaments no autoritzats. I això amb independència que es tracti del seu propi personal o bé de terceres persones alienes a l'IMSS.

El compliment d'aquesta obligació que imposa l'RGPD pot justificar el tractament de determinades dades personals per part de l'IMSS.

Segons es desprèn del contracte d'encarregat del tractament subscrit entre l'ATM i l'IMSS, adjuntat a l'escrit de consulta, l'IMSS ha autoritzat que els treballadors de TMB que tenen assignades funcions de gestió i tramitació de la targeta bonificada per a persones en situació d'atur puguin accedir al seu sistema d'informació SIAS, per tal de poder consultar, en el si del seu procediment d'expedició, si la persona que sol·licita la targeta en pot ser o no beneficiària (acord 1r). La informació a què podran accedir aquests treballadors comprèn la verificació (positiva o negativa) del compliment dels requisits exigits per poder adquirir la targeta bonificada. TMB actuaria, respecte el tractament d'aquestes dades, com a subencarregat del tractament (acord 4t).

D'acord amb les manifestacions efectuades en l'escrit de consulta, aquest accés al sistema SIAS del personal autoritzat de TMB (agents d'informació i atenció ciutadana) es produeix a través de la introducció del seu número de DNI.

No és clar, de la informació facilitada, si aquesta dada és la única que s'empra per accedir al sistema SIAS. Si fos aquest el cas, cal dir que la identificació només a través d'un usuari no sembla prou segura, atès que no garanteix l'autenticació, això és no permet tenir la certesa que la persona que intenta accedir al sistema d'informació és qui realment diu ser. Però especialment resulta poc fiable si l'usuari atorgat coincideix amb el número de DNI.

Amb caràcter general, s'ha de reconèixer que, malgrat que el número de DNI no és un número d'identificació destinat a ésser de públic coneixement, malauradament sovint apareix publicat -en ocasions sense base legal- en instruments de diferent naturalesa (diaris oficials, webs, etc.). Si bé aquesta Autoritat ha advertit, en diverses ocasions, dels efectes perniciosos d'aquesta pràctica, el cert és que a dia d'avui encara hi ha molts números de DNI que resulten fàcilment accessibles. Per tant, utilitzar el número de DNI com a únic identificador per poder accedir a un sistema d'informació on només determinades persones haurien de tenir capacitat per accedir-hi no resultaria una mesura de seguretat adequada.

Qüestió diferent és que s'empri aquesta dada relativa al número de DNI per identificar-se com a usuari del sistema SIAS i es combini aquesta informació amb un sistema d'autenticació basat en l'existència de contrasenyes.

Aquest tipus de mecanisme d'identificació i d'autenticació (usuari i contrasenya) és el mètode més estès per impedir accessos no autoritzats vers sistemes o continguts dins un sistema d'informació. Es tracta d'una mesura establerta en estàndards internacionals i en certificacions en matèria de seguretat informàtica (com ara, la Norma ISO/IEC 27001 sobre la gestió de la seguretat de la informació) i també reconeguda pel nostre ordenament jurídic.

Així, per exemple, la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (en endavant, LPACAP), disposa 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**.*
> *(…)".*

Per la seva part, l'article 93 de l'RLOPD -aplicable en allò que no s'oposi a l'RGPD- també establia que el responsable havia d'establir un mecanisme que permetés la identificació inequívoca de qualsevol usuari que intentés accedir a un sistema d'informació i també verificar que estigués autoritzat. En aquest sentit, admetia l'ús de mecanismes d'autenticació basats en l'existència de contrasenyes.

Així doncs, pot dir-se que, amb caràcter general, la utilització d'un usuari i d'una contrasenya com a mecanisme d'identificació i d'autenticació per accedir a un determinat sistema d'informació es considera una mesura de seguretat adequada. Això, sens perjudici que, en atenció al risc que comporti el tractament de la informació de què es tracti, pugui resultar necessari establir altres tipus de mecanismes més robustos (per exemple, basats en certificats electrònics, etc.).

V

Partint de la premissa que en el present cas l'accés al sistema d'informació SIAS per als treballadors de (...) que tenen encomanada la tramitació i l'expedició de la targeta bonificada per a persones en situació d'atur s'efectua a través d'un mecanisme d'identificació i d'autenticació basats en un usuari i una contrasenya, cal examinar específicament si l'ús de la dada relativa al número de DNI com a usuari resulta adequat des del punt de vista de la protecció de dades.

L'article 5 de l'RGPD, ja citat, disposa 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»);
(...)".

Des del punt de vista de la gestió dels sistemes d'informació, el nom d'usuari respon a la pregunta ¿qui ets?. Tenint en compte això i la necessitat de garantir que no es produiran accessos no autoritzats, és clar que ha de reunir una característica fonamental: ha d'ésser únic.

En aquest sentit, i en atenció al context en què ens trobem (accés a informació personal emmarcat en el si d'un procediment administratiu) el nom i cognoms (identificació directa) o un número d'identificació personal (identificació indirecta) serien probablement les dades personals més adequades.

En funció de la dimensió i l'estructura de l'organització o llur naturalesa, la gestió dels noms d'usuari pot ésser un procés laboriós. Així, per exemple, la utilització del nom propi de la persona autoritzada per accedir al sistema com a nom d'usuari pot ésser una opció viable en un ens petit, però no així en un organisme de mitjana o gran dimensió. En organitzacions amb estructures ben definides pot ésser d'utilitat afegir-hi un codi, per exemple el codi del departament, com a part del nom d'usuari. En d'altres ocasions, les característiques pròpies del treball que du a terme el personal autoritzat pot requerir preservar la seva identitat, com ara, per motius de seguretat personal, per tant, la utilització d'un número d'identificació personal específic podria ser preferible en aquests casos. En d'altres, també cal autoritzar accessos per personal aliè al de la pròpia organització. Sigui com sigui, una correcta gestió dels comptes d'usuaris obliga, en qualsevol cas, a vetllar per a que els noms d'usuaris emprats no coincideixin, evitant així el risc d'un accés per persones no autoritzades o a informació personal indeguda.

El Reial decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica, disposa 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."

Atès que el DNI és el document creat expressament per acreditar inequívocament la identitat de la persona que el posseeix podria dir-se que s'erigeix com un mecanisme òptim en termes d'identificació d'usuaris.

Prova d'això és que el legislador l'ha triat com el mecanisme d'identificació electrònica dels ciutadans que en tot cas ha d'ésser admès per les administracions públiques quan aquests s'hi relacionen per mitjans electrònics.

També cal tenir present que l'LPACAP estableix, en el seu article 9.1, ja citat, que el DNI és el document a través del qual les administracions públiques han de verificar la identitat de les persones interessades en el procediment administratiu.

Així doncs, si bé no és imprescindible que el nom d'usuari d'un sistema d'informació coincideixi amb el número de DNI de la persona autoritzada per accedir-hi, no pot dir-se que, des del punt de vista de la protecció de dades, resulti una dada personal inadequada o no pertinent, atès que la seva utilització certament permet assolir la finalitat per a la qual es tracta en el present cas, això és garantir de manera inequívoca la identitat de la persona usuària del sistema d'informació.

Per tant, amb caràcter general, podria dir-se que el seu tractament s'adequaria al principi de minimització de dades (article 5.1.c) RGPD).

VI

En l'escrit de consulta, també es planteja quina és la base legal que legitimaria la comunicació de la dada relativa al número del DNI dels treballadors de TMB vers l'IMSS.

Com s'ha vist, l'RGPD obliga (...) a adoptar les mesures tècniques necessàries per evitar tractaments no autoritzats (articles 5.1.f), 24 i 32), per tant, a vetllar perquè només les persones legitimades puguin tenir accés al seu sistema SIAS i només a les dades personals que, en cada cas, resultin estrictament necessàries (article 5.1.c) RGPD).

En el present cas existeix un contracte d'encarregat del tractament entre l'IMSS i l'ATM subscrit per establir un mecanisme de col·laboració i cooperació entre ambdues entitats per tal de facilitar la tramitació de la targeta bonificada per a aquelles persones residents al municipi que, rebent algun tipus d'ajut dels serveis socials de l'Ajuntament, en podrien ésser beneficiàries.

El desenvolupament i l'execució d'aquest encàrrec comporta que els diferents operadors del transport públic hagin de poder consultar determinada informació personal en poder de l'IMSS. Per aquest motiu, l'IMSS autoritza expressament l'ATM a subencarregar el tractament de les dades personals vinculades o relacionades amb la tramitació d'aquest títol de transport bonificat als dits operadors, entre ells, TMB.

En virtut d'aquest subencàrrec del tractament (article 28.4 RGPD), el personal de (...) que tingui expressament assignades funcions de tramitació dels diferents títols de transport integrat estarà legitimat per accedir al sistema SIAS.

Per tal de fer efectiu aquest accés (per establir-ne els corresponents permisos d'accés al SIAS), l'IMSS requereix que TMB li comuniqui per avançat quines són aquestes persones (segons la informació aportada els agents d'informació i atenció ciutadana).

En la mesura, per tant, que la comunicació del número de DNI dels treballadors de TMB vers l'IMSS tindria per finalitat identificar aquelles persones del seu personal que, en atenció a les funcions que tenen assignades en virtut del seu contracte laboral (article 20 ET), han de poder accedir al sistema SIAS per poder gestionar de manera efectiva la tramitació de la targeta bonificada, el tractament d'aquesta dada (la comunicació del número de DNI) podria considerar-se emparat en el marc de l'execució d'un contracte, en base a allò disposat a l'article 6.1.b) de l'RGPD.

Dit això, fer avinent que el contracte d'encàrrec del tractament subscrit entre l'IMSS i l'ATM hauria d'ésser objecte de revisió als efectes d'adequar-lo a les previsions de l'article 28.3 de l'RGPD. En aquest sentit, pot ser d'interès consultar la Guia sobre l'encarregat del tractament a l'RGPD elaborada per les autoritats de protecció de dades per ajudar els responsables i els encarregats en l'adaptació a les exigències de l'RGPD, disponible al web de l'Autoritat http://apdcat.gencat.cat/ca/inici/.

D'acord amb les consideracions fetes fins ara en relació amb la consulta plantejada, es fan les següents,

Conclusions

L'establiment per l'IMSS d'un mecanisme d'identificació i d'autenticació basat en l'ús d'un usuari -consistent en el número de DNI- i d'una contrasenya per a aquells treballadors de TMB que, en virtut de la seva condició de personal d'un subencarregat del tractament, han de poder accedir al sistema SIAS per exercir les funcions que tenen encomanades (tramitació de la targeta bonificada per a les persones en situació d'atur), podria considerar-se una mesura de seguretat adequada, amb base jurídica a l'article 6.1.b) de l'RGPD, atès que és necessari per a l'execució del contracte.

Barcelona, 18 de juliol de 2018