Opinion in relation to a query about the use of the DNI number to access a council's information system

A letter is presented to the Catalan Data Protection Authority in which it is considered whether the use of the DNI number to access a City Council information system, for the purposes of processing the subsidized card for people in a situation of 'atur, complies with the legislation on the protection of personal data.

A copy of the data processor contract signed between the Metropolitan Transport Authority and the City Council's Municipal Institute of Social Services is attached to the consultation letter.

Having analyzed the request and the documentation that accompanies it, and having seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

(...) states, in its consultation letter, that the Metropolitan Transport Authority (hereafter, ATM) agreed to expand the people who can be beneficiaries of the subsidized card for people in a situation of unemployment to those people who, despite not receiving any aid from the State, receive aid from the social services of the councils integrated within the scope of the ATM.

He then explains that, in order to facilitate the management and processing of this subsidized card for people who receive aid from the City Council's social services, a processing contract was signed between the ATM and the ATM Municipal Institute of Social Services (IMSS), of which a copy is attached.

It should also be noted that, by virtue of this contractor contract, the IMSS expressly authorizes the ATM to subcontract the processing of personal data subject to the contract to transport operators - among which is Transports Metropolitans de Barcelona (hereinafter, TMB)-, given that access to the data for them is considered essential for the effective implementation of the service and for the management of the corresponding transport tickets and their beneficiaries.

Having said that, he explains that the IMSS makes the SIAS application available to TMB employees, so that, during the process of processing the subsidized card, they can check whether or not the person requesting it can be a beneficiary . In particular, it points out that workers' access to this IMSS application is carried out by entering the DNI number.

(...) poses the following questions to this Authority:

a) If the data requested to access the SIAS system (DNI number of the TMB information and citizen attention agents) are proportionate in terms of their purpose and, consequently, if the employee can be required to your access to the system as

user through his ID and if this requirement is respectful of the principles that govern the protection of personal data.

b) In any case, what can be understood to be the legal basis of the described treatment (communication of the ID number of certain TMB employees to the City Council through the SIAS database).

These issues are examined in the following sections of this opinion.

First, please note that, in view of the data controller contract provided, the considerations made throughout this opinion are applicable only to TMB staff but would not cover other staff who do not meet this condition.

III

The Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereafter, RGPD), fully applicable since the last May 25 (article 99), establishes that all processing of personal data must be lawful (article 5.1.a)) and, in this sense, establishes a system of legitimizing the processing of data which is based on the need for one of the legal bases established in its article 6, which do not maintain any relationship of priority or precedence.

The aforementioned article 6.1 of the RGPD provides, specifically, that:

"1. The treatment will only be lawful if at least one of the following conditions is met: a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes; b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures; c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment; d) the treatment is necessary to protect the vital interests of the interested party or another natural person; e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment; f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child.

The provisions in letter f) of the first paragraph shall not apply to the processing carried out by public authorities in the exercise of their functions."

For its part, article 6.3 of the RGPD provides that the basis of the treatment indicated in sections c) and e) of this article 6.1 of the RGPD must be established by Union Law European or by the law of the Member States that applies to the data controller.

Despite the fact that recital 41 of the RGPD provides that "when the present Regulation makes reference to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament", it must be taken into account that the same recital establishes that this "without prejudice to the requirements in accordance with the constitutional order of the Member State in question".

The referral to the legitimate basis established in accordance with the internal law of the member states referred to in article 6.3 of the RGPD requires, in the case of the Spanish State, that the development rule, to be a fundamental right, has the status of law (Article 53 EC).

In this sense, the Draft Organic Law on the Protection of Personal Data, approved by the Council of Ministers on November 10, 2017 (BOCG, series A, no. 13-1, of 24.11.2017), although for reasons obviously not applicable, establishes:

> "Article 8. Data treatment protected by law.
> 1. The processing of personal data can only be considered based on the fulfillment of a legal obligation required of the person in charge, in the terms provided for in article 6.1 c) of Regulation (EU) 2016/679, when this is provided for by a rule of European Union law or a law, which may determine the general conditions of the treatment and the types of data subject to it as well as the assignments that proceed as a consequence of the fulfillment of the legal obligation. The law may also impose special conditions on treatment, such as the adoption of additional security measures or others established in Chapter IV of Regulation (EU) 2016/679.
>
> 2. The treatment of personal data can only be considered based on the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible, in the terms provided for in article 6.1 e) of Regulation (EU) 2016 /679, when it derives from a competence attributed by law."

Therefore, to consider the data treatments covered by the legal bases of article 6.1.c) i) of the RGPD there must be a regulatory provision with the rank of law.

Law 12/2007, of 11 October, on social services, establishes that:

> "Article 27
> Public responsibilities 1. The
> Administration of the Generalitat, the municipalities and the other local bodies of Catalonia are the competent administrations in the matter of social services, in accordance with the provisions of this title and, where appropriate, the legislation on territorial organization and local regime.
> 2. Municipalities and other local bodies may exercise powers belonging to the Administration of the Generalitat by way of delegation, management assignment or joint management formulas, without prejudice to the powers attributed to them by law."

Article 31 of this same Law, to which we refer, determines the competences that correspond to the municipalities in the matter of social services.

For its part, the Barcelona Municipal Charter, approved by Law 22/1998, of December 30, determines the powers that, among other matters, correspond specifically to the municipality of Barcelona in the matter of social services (Title VI , Chapter X).

The IMSS is the autonomous body created by the City Council to promote, organize and articulate the basic social care services of municipal responsibility aimed at all people who reside in this city.

In view of these forecasts, it can be said that, in general, the processing of personal data carried out by the IMSS in compliance with the obligations established in Law 12/2007 responds to the exercise of "a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment", so they would be legitimated by article 6.1.e) of the RGPD.

IV

Having said that, it must be borne in mind that the processing of this data by the IMSS must also comply with the rest of the principles established in the RGPD, especially, for the purposes that are of interest in the present case, at the beginning of integrity and confidentiality.

Article 5 of the RGPD establishes that:

> "1. The personal data will be: (...) f)
> treated in such a way as to
> guarantee an adequate security of the personal data, including protection against unauthorized or illegal treatment and against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality")."

Regarding this, article 24 of the RGPD provides that:

> "1. Taking into account the nature, the scope, the context and the purposes of the treatment as well as the risks of varying probability and severity for the rights and freedoms of the physical persons, the person responsible for the treatment will apply appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the treatment complies with this Regulation. These measures will be reviewed and updated when necessary. (…)".

It should be taken into account, therefore, that the RGPD imposes the obligation on the data controller to adopt the necessary technical and organizational measures to guarantee the security of the personal data that will be processed. Obligation which, it must be said, also extends to the person in charge of the treatment (Article 28.3.c) RGPD) and, where appropriate, sub-processor (Article 28.4 RGPD).

Point out, at this point, that the RGPD sets up a security system that is not based on the basic, medium and high security levels provided for in the Implementing Regulation of Organic Law 15/1999, of December 13, of protection of personal data, approved by Royal Decree 1720/2007, of December 21 (RLOPD), but by determining, following a prior risk assessment, which security measures are necessary in each case (Recital 83 and article 32).

Therefore, the scheme of security measures provided for in the RLOPD cannot, since last May 25, be considered valid automatically. In some cases, these same measures may continue to be applied if it is concluded from the previous risk analysis that the measures are really the most suitable to offer a level of security appropriate to the specific case, but in others it may be necessary to complete them with additional measures.

Also agreeing that, in the case of public administrations, the application of security measures will be marked by the criteria established in the National Security Scheme, approved by Royal Decree 3/2010, of January 8, which, currently , is being reviewed.

In this sense, the LOPD Project, mentioned above, provides that:

> "First additional provision. Security measures in the public sector.
>
> The National Security Scheme will include the measures that must be implemented in case of processing of personal data, to avoid its loss, alteration

or unauthorized access, adapting the criteria for determining the risk in data processing to that established in article 32 of Regulation (EU) 2016/679."

In any case, in accordance with these precepts, it is clear that the IMSS is responsible for the implementation of these security measures regarding the data processing for which it is responsible.

In the present case and based on the information available, the IMSS is responsible for the SIAS information system, which contains the personal data of the users of the municipal social services.

It is therefore up to the IMSS, among other actions in the field of security, to determine which people must access and process the personal information contained in this information system, as well as to adopt appropriate mechanisms that allow its correct identification and authentication as users of the system, in order to guarantee, as required by the RGPD, that no unauthorized treatments will occur. And this regardless of whether it is their own staff or third parties outside the IMSS.

Compliance with this obligation imposed by the RGPD may justify the processing of certain personal data by the IMSS.

As can be seen from the processor contract signed between the ATM and the IMSS, attached to the consultation letter, the IMSS has authorized the TMB workers who are assigned the functions of managing and processing the bonus card for unemployed people to be able to access their SIAS information system, in order to be able to check, as part of the issuing procedure, whether or not the person applying for the card can be a beneficiary (1st agreement). The information that these workers will be able to access includes the verification (positive or negative) of compliance with the requirements required to be able to purchase the bonus card. TMB would act, with respect to the processing of this data, as sub-processor (4th agreement).

According to the statements made in the consultation letter, this access to the SIAS system by the authorized staff of TMB (information agents and citizen attention) occurs through the introduction of their ID number.

It is not clear, from the information provided, if this data is the only one used to access the SIAS system. If this were the case, it must be said that identification only through a user does not seem secure enough, given that it does not guarantee authentication, that is, it does not allow us to be certain that the person trying to access the information system is who he really says he is. But it is especially unreliable if the granted user matches the ID number.

In general, it must be recognized that, despite the fact that the DNI number is not an identification number destined to be public knowledge, unfortunately it often appears published - sometimes without a legal basis - in instruments of a different nature (official newspapers , websites, etc.). Although this Authority has warned, on several occasions, of the pernicious effects of this practice, the truth is that today there are still many DNI numbers that are easily accessible. Therefore, using the DNI number as the only identifier to be able to access an information system where only certain people should have the ability to access it would not be an adequate security measure.

It is a different matter that this data relating to the ID number is used to identify itself as a user of the SIAS system and that this information is combined with an authentication system based on the existence of passwords.

This type of identification and authentication mechanism (user and password) is the most widespread method to prevent unauthorized access to systems or content within an information system. This is a measure established in international standards and in IT security certifications (such as the ISO/IEC 27001 Standard on information security management) and also recognized by our legal system.

Thus, for example, Law 39/2015, of October 1, on the common administrative procedure of public administrations (hereafter, LPACAP), provides that:

> "Article 9. Identification systems of those interested in the procedure.
> 1. The Public Administrations **are obliged to verify the identity** of those interested in the administrative procedure, by checking their name and surname or denomination or company name, as appropriate, which are contained in the **National Identity** Document or equivalent identification document.
> 2. Those interested **may identify themselves electronically** before the Public Administrations through any system that has a previous registration as a user that allows their identity to be guaranteed. In particular, the following systems will be admitted: a) Systems based on recognized or qualified electronic certificates of electronic signature issued by providers included in the "Trusted list of providers of certification services". For these purposes, recognized or qualified electronic certificates are understood to include those of legal persons and entities without legal personality. b) Systems based on recognized or qualified electronic certificates issued by providers included in the "Trusted list of certification service providers". c) Coordinated key systems and **any other system that the Public Administrations consider valid, under the terms and conditions that are established.** (…)".

For its part, article 93 of the RLOPD - applicable where it is not opposed to the RGPD - also established that the person in charge must establish a mechanism that allows the unequivocal identification of any user who tries to access an information system and also verify that it was authorized. In this sense, it supported the use of authentication mechanisms based on the existence of passwords.

So, it can be said that, in general, the use of a user and a password as an identification and authentication mechanism to access a certain information system is considered an adequate security measure . This, without prejudice to the fact that, in view of the risk involved in the treatment of the information in question, it may be necessary to establish other types of more robust mechanisms (for example, based on electronic certificates, etc.).

v

Based on the premise that in the present case the access to the SIAS information system for the workers of (...) who are entrusted with the processing and issuing of the bonus card for people in a situation of unemployment is carried out through an identification and authentication mechanism based on a user and a password, it is necessary to specifically examine whether the use of the data relating to the DNI number as a user is appropriate from the point of view of protection of data

Article 5 of the RGPD, already cited, provides that:

"1. The personal data will be:
(...) c) adequate, relevant and
limited to what is necessary in relation to the purposes for which they are treated
("minimization of data"); (...)".

From the point of view of the management of information systems, the user name answers the question "Who are you?". Considering this and the need to ensure that unauthorized access will not occur, it is clear that it must meet one fundamental characteristic: it must be unique.

In this sense, and paying attention to the context in which we find ourselves (access to personal information framed within an administrative procedure) the name and surname (direct identification) or a personal identification number (indirect identification) would probably be the more appropriate personal data.

Depending on the size and structure of the organization or their nature, managing usernames can be a laborious process. Thus, for example, the use of the name of the person authorized to access the system as a user name may be a viable option in a small organization, but not so in a medium or large organization. In organizations with well-defined structures it may be useful to add a code, for example the department code, as part of the user name. On other occasions, the specific characteristics of the work carried out by the authorized personnel may require preserving their identity, such as for reasons of personal security, therefore the use of a specific personal identification number could be preferable in these cases. In others, it is also necessary to authorize access by personnel other than those of the organization itself. Be that as it may, correct management of user accounts requires, in any case, to ensure that the usernames used do not match, thus avoiding the risk of unauthorized access or improper personal information.

Royal Decree 1553/2005, of 23 December, which regulates the issuance of the national identity document and its electronic signature certificates, provides that:

"Article 1. Nature and functions.
1. **The National Identity Document is a personal and non-transferable document** issued by the Ministry of the Interior that enjoys the protection granted by law to public and official documents. Its owner will be obliged to keep and conserve it.

2. Said Document **has sufficient value, on its own, to prove identity and the personal data of its holder that are recorded in it,** as well as its Spanish nationality.
3. **Each National Identity Document will be assigned a personal number that will be considered a general personal numerical identifier.**

4. **Equally, the National Identity Document allows Spaniards who are of age and who enjoy full capacity to create the electronic identification of its holder,** as well as to perform the electronic signature of documents, in the terms provided for in Law 59/2003 , of December 19, electronically signed.
In the case of Spanish minors, or those who do not enjoy full capacity to work, the national identity document will only contain the utility of the electronic identification, issued with the respective certificate of authentication activated.

5. The electronic signature made through the National Identity Document will have the same value with respect to the data entered in electronic form as the handwritten signature in relation to the data entered on paper.

6. No Spaniard may be deprived of the National Identity Document, not even temporarily, except in the cases and form established by the Laws in which it must be replaced by another document."

Given that the DNI is the document created expressly to unequivocally accredit the identity of the person who owns it, it could be said that it stands as an optimal mechanism in terms of user identification.

Proof of this is that the legislator has chosen it as the electronic identification mechanism for citizens that must in any case be accepted by public administrations when they relate to it by electronic means.

It should also be borne in mind that the LCAPAP establishes, in its already cited article 9.1, that the DNI is the document through which the public administrations must verify the identity of the persons interested in the administrative procedure.

So, while it is not essential that the user name of an information system matches the ID number of the person authorized to access it, it cannot be said that, from the point of view of data protection, it turns out to be inadequate or irrelevant personal data, given that its use certainly allows to achieve the purpose for which it is treated in the present case, that is to unequivocally guarantee the identity of the user of the system information

Therefore, in general, it could be said that its treatment would comply with the principle of data minimization (Article 5.1.c) RGPD).

VI

In the consultation letter, it is also considered what is the legal basis that would legitimize the communication of the data relating to the DNI number of TMB workers to the IMSS.

As we have seen, the RGPD obliges (...) to adopt the necessary technical measures to avoid unauthorized treatment (articles 5.1.f), 24 and 32), therefore, to ensure that only authorized persons can have access to your SIAS system and only to the personal data that, in each case, are strictly necessary (article 5.1.c) RGPD).

In the present case there is a processing contract between the IMSS and the ATM signed to establish a collaboration and cooperation mechanism between both entities in order to facilitate the processing of the bonus card for those residents of the municipality that, receiving some type of aid from the City Council's social services, could be beneficiaries.

The development and execution of this order means that the different public transport operators must be able to consult certain personal information held by the IMSS. For this reason, the IMSS expressly authorizes the ATM to subcontract the processing of personal data linked or related to the processing of this subsidized transport ticket to the said operators, including TMB.

By virtue of this processing sub-task (article 28.4 RGPD), the staff of (...) who have been expressly assigned processing functions for the various integrated transport tickets will be authorized to access the SIAS system.

In order to make this access effective (to establish the corresponding access permissions to SIAS), the IMSS requires TMB to inform it in advance who these people are (according to the information provided by the information and public attention agents) .

To the extent, therefore, that the communication of the DNI number of TMB workers to the IMSS would have the purpose of identifying those persons of its staff who, in attention to the functions assigned to them by virtue of their employment contract (article 20 ET), they must be able to access the SIAS system to be able to effectively manage the processing of the bonus card, the processing of this data (the communication of the ID number) could be considered protected in the framework of the execution of 'a contract, based on what is provided in article 6.1.b) of the RGPD.

Having said that, it should be agreed that the treatment contract signed between the IMSS and the ATM should be subject to review for the purposes of adapting it to the provisions of article 28.3 of the RGPD. In this regard, it may be of interest to consult the Guide on the Data Controller in the RGPD prepared by the data protection authorities to assist controllers and processors in adapting to the requirements of the RGPD, available on the Authority's website http://apdcat.gencat.cat/ca/inici/.

In accordance with the considerations made so far in relation to the query raised, the following are made,

Conclusions

The establishment by the IMSS of an identification and authentication mechanism based on the use of a user -consisting of the DNI number- and a password for those TMB workers who, by virtue of their personal status of a sub-processor, they must be able to access the SIAS system to carry out the functions entrusted to them (processing of the bonus card for people in a situation of unemployment), it could be considered a measure of adequate security, with a legal basis in article 6.1.b) of the RGPD, given that it is necessary for the execution of the contract.

Barcelona, July 18, 2018