CNS 39/2020

Opinion in relation to the query made by a public administration on qualified certificates for public workers

A letter from (...) is submitted to the Catalan Data Protection Authority in which it is requested that the Authority issue an opinion on the suitability of the qualified certificates for public workers who issued by the Consortium of the Open Administration of Catalonia (hereafter, AOC).

Having analyzed the request and seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

The entity states in its consultation that the inclusion of the DNI data in the qualified certificates issued to public workers from the AOC constitutes data processing that would not comply with data protection regulations, when dealing with - of information that is not necessary for the purposes of identifying the authorities and staff at the service of public administrations.

It also points out that this Authority, on several occasions, has stated that the dissemination of electronically signed documents using this type of certificate entails, given its configuration, the dissemination of unnecessary personal identifying data that must be avoided.

On this issue, the entity considers that the solution proposed to minimize the dissemination of the DNI consisting of modifying the configuration of the image generated in the electronic signature is not an effective mechanism, given that this information is accessible by consulting the properties of the signature.

For all this, the entity requests to know the planned actions to resolve these situations

III

It should be noted that the problem raised in the present consultation is a matter on which this Authority has already pronounced previously, in particular, in opinion CNS 17/2017, which is available on the website https://apdcat. gencat.cat/ca/inici, to which we refer.

However, it is not superfluous, for the purposes that are of interest, to recall, briefly, the main considerations:

- In accordance with the principle of data minimization (Article 5.1.c) Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection Regulation (RGPD)), the data of public workers included in the configuration of the certificates

Qualified electronic signatures must be the minimum necessary to fulfill the intended purpose.

Mainly dealing with the identification of the public worker who signs a certain administrative document (article 53.1.b) of Law 39/2015, of October 1, on the common administrative procedure of public administrations), this Authority considers (FJ III) that it is sufficient, from the point of view of the principle of minimization, to provide his name, surname and position, given that this is the minimum necessary personal information required by the citizen to know the identity of the person who has served in his performance before the Public Administration.

Having said that, it is also necessary to adhere to the forecasts established in the sectoral regulations that apply.

- The certificates for public workers issued by certification service providers, including the AOC, must comply with the provisions of Law 59/2003, of December 19, on electronic signatures (LSE) , as well as Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, relating to electronic identification and trust services for electronic transactions in the internal market (ReIDAS).

Article 11.1 of the LSE establishes that *"electronic certificates issued by a certification service provider that meets the requirements established in this law regarding the verification of the identity and other circumstances of the applicants and the reliability are recognized certificates and the guarantees of the certification services they provide."*

According to this law, these certificates must include, among other information, *"the identification of the signatory, in the case of natural persons, by their name and surname and their* ***national identity document number*** *or through a pseudonym that appears as such unequivocally and, in the case of legal entities, by its denomination or corporate identity and its fiscal identification code" (article* 11.2.e) LSE).

For its part, ReIDAS establishes that the identification of the person signing in the configuration of the qualified certificate of electronic signature is done by indicating ***"at least the number of the signatory or a pseudonym" (annex*** I, letter c)). And it expressly provides (article 28) that these certificates ***"will not be subject to any mandatory requirement*** *that exceeds the requirements established in annex I" (section* 2), although it also provides that *"they may include additional non-mandatory specific attributes",* always that these attributes do not affect *"the* ***interoperability*** *and recognition of qualified electronic signatures" (section* 3).

In view of these forecasts, and taking into account that the European Regulations are mandatory in all their elements and directly applicable to the Member States (Article 288 TFEU), this Authority considers (FJ V) that the requirement to include the number of DNI in the certificates, referred to by the LSE, could only be considered valid, with regard to ReIDAS, to the extent that this data was incorporated as an additional non-mandatory specific attribute and as long as doing so did not compromise interoperability and the recognition of the qualified electronic signature.

- The syntactic structure and the content of the fields of the certificates for public workers issued by the AOC are defined in the "certificate profile" document, prepared by the requirements of the LSE (article 19), following the parameters established by the Ministry of Finance and Public Administrations (MHAP).

In accordance with the criteria for the composition of the CN *(Common Name)* field contained in the MHAP *"Profiles of Electronic Certificates"* document (April 2016 edition), the inclusion of the DNI number in the certificates is mandatory (section 10.1).

Considering that ReIDAS only establishes the inclusion of the signatory's name (annex I) and the allocation of any other information (as could be the case of the DNI) would remain limited to the extent that this allocation was not mandatory (article 28.2) and the fact that the interoperability of the qualified signature was not compromised (article 28.3), the Authority considers (FJ VI) that the establishment of this criterion for qualified public worker certificates, of necessarily including the DNI in the CN field, would be, at the very least, questionable in relation to the forecasts of the ReIDAS.

In any case, in view of the provisions established in the *ETSI EN 319 412-2 standard Certificate profile for certificates issued to natural persons,* which supports the requirements of the qualified certificates required in the ReIDAS (and to which the aforementioned document also refers of the MHAP), the Authority considers (FJ VI) that the inclusion of the DNI number in the CN field of qualified public worker certificates would not be relevant or necessary, for the purposes of identifying the person signing. What's more, given that ReIDAS does not prevent the issuance of qualified certificates of electronic signature with a pseudonym, it could even be understood that the inclusion of the DNI in any of the fields of the certificate's profile would not be necessary.

Given this, the Authority believes that the inclusion of the DNI number in the qualified public worker certificates could respond not only to the desire to guarantee the identity of the person signing, but to the need to guarantee interoperability between the applications that they use them, although in this case it is considered that the CN field might not be the most appropriate option for that purpose.

For all that, the Authority concludes (FJ VI) that, from the point of view of the minimization principle, as long as interoperability was not affected, the inclusion of the DNI in the qualified public worker certificates would not be justified.

At the date of issuance of this opinion, this continues to be the criterion supported by this Authority.

IV

The entity raises in the consultation what actions have been planned to adapt the issuance of qualified public worker certificates to the data protection regulations.

As was agreed in the aforementioned opinion CNS 17/2017, from the point of view of the right to data protection, for the purposes of avoiding the dissemination of the data relating to no. of ID, it is necessary to assess the possibility of establishing a certification policy that foresees the use of qualified certificates of public workers based on pseudonyms.

The Authority considered - and considers - that the use of pseudonyms is a fully valid option in view of the ReIDAS forecasts examined (FJ VII):

> *"Given, precisely, the forecasts of the ReIDAS on the use of pseudonyms, for the purposes to avoid the unnecessary dissemination of personal data of public workers in the signature of electronic documents, as a result of the configuration of the certificates qualified, the option of using pseudonyms could be considered in a case such as the one examined in a generalized way.*
>
> *This possibility, although it could be conflicting in attention to the provisions of the Law 40/2015 (article 43.2 allows limiting the identification data of the worker in the certificate, using instead the professional identification number, but only for*

reasons of public security), is fully applicable in accordance with Annex I of REIDAS.

It should be remembered that each organization providing certification services can establish its own own declaration of certification practices and define, therefore, the profiles of the certificates that issues (article 19 LSE).

So, the AOC Consortium could establish, in the qualified certificate profile of public worker, that the identification of the person signing will be carried out, with general character, through a pseudonym. This pseudonym could be the name and surnames of the public worker and, where appropriate, position or category, provided that, for reasons of public safety, it is not required to preserve your anonymity. This way the dissemination of the DNI data that could be included in any of the information fields that make up the structure of the certificate would be avoided.

If, certainly, for reasons of public security, anonymity should be guaranteed of the public worker, the pseudonym could be his professional identification code, en insofar as this is not related to personal data of the public employee (such as the ID number), or any other indicator provided by the Administration public in which it provides its services.

In both cases it should be clearly indicated that it is a pseudonym (annex I ReIDAS).”

Beyond this, the adoption of the appropriate actions to avoid the processing of personal data that may not be necessary from the point of view of the minimization principle (Article 5.1.c) RGPD) in the issuance of the certificates of public worker is a question that can correspond to the current Ministry of Finance, the Ministry of Economic Affairs and Transformation
Digital, and to the various certification service providers.

v

The entity also agrees in the consultation that the proposed solution, in order to minimize the dissemination of the no. of DNI following the publication of documents that incorporate an electronic signature, consisting of modifying the appearance of the signature, is not an effective mechanism, given that this information is accessible by consulting the properties of the signature.

As the query points out, this Authority has stated on several occasions (in opinion CNS 17/2017, already cited, and also, among others, in opinion CNS 23/2017, CNS 58/2018, CNS 1/2019 or CNS 12/2020) that, when a certain document is signed electronically
through the public worker certificate, there is certain personal information of this worker that is accessible to those people who have access to said document
(name, surname, ID number and position of the worker, among other information).

Also that, taking into account that the intended purpose with the incorporation of said signature may be related, mainly, to the right of the interested parties to identify the authorities and the
personnel at the service of the public administrations under whose responsibility it is
process certain procedures or disseminate certain documents (article 53.1.b)
LPACAP), it is considered justified that the name and surname of the person who signs it, including the position, may appear in the document, but not their ID number (article 5.1.c) RGPD).

And this Authority has also maintained that, beyond the possibility that exists to configure the appearance of the signature that appears printed on the document and that already allows to avoid certain unnecessary information at a first level of dissemination, the truth is that the possibility of access the

properties of the certificate used to sign allows access to some unnecessary data, such as that relating to the ID of the person signing.

For this reason, the Authority proposes (CNS opinion 1/2019), in a case linked to the publication of documents, different options to avoid access to the DNI number contained in the properties of the certificate with which it has been signed the document, which are transcribed below (FJ V):

"Option A: Evaluate the convenience of carrying out the publication of the documents, for the purposes of transparency of the contractual activity of the public administrations, without incorporating said signatures.

Option B: If you want to keep the electronic signature visible, publish an "image" of the document in question (not the document in its original format) in which, as data of the signatory, only the name, surname and position are included. For this purpose, it would be necessary:

1. Define the appearance of the signature of the public worker in such a way that only the data relating to the name, surname and position are "visible".

Keep in mind that the appearance or image of a certificate-based signature is something that a priori can be previously defined through the options that, in this sense, offers the program used to sign electronically (eg Adobe Acrobat), so the data of the public worker that are incorporated in the electronic certificate does not necessarily have to be visible once it has been signed electronically the document. The visibility or not of these personal data will depend, therefore, in the manner in which the format of said signature has been pre-established. And this regardless of the type of electronic certificate that the worker has.

Thus, in relation to the new qualified certificates for public workers, in which, following the parameters established by the Ministry of Finance and Public Administrations, in order to adapt to Regulation (EU) 910/2014 of the European Parliament and of the Council, of July 23, 2014, relating to electronic identification and trust services for electronic transactions in the internal market, the worker's name, surname and DNI data are incorporated together in the Common Name field of the certificate - therefore, showing this field in the image of the signature would spread excessive data (DNI) - it would be necessary to create a new aspect of this signature in which only the name, surname and position data would be incorporated.

2. Convert the document to be published to "image" format (for example, by scanning it).

It should be noted that modifying the appearance or format of the signature image is not it really prevents "access" to the personal information of the signatory that is included in the configuration of your public worker certificate. This information - that only could be modified by the certification service provider - it is accessible to by querying the signature properties. Now, if the document is published in "image" format, the possibility of accessing these properties of the certificate and, therefore, the worker's ID card is eliminated."

Subsequently, and in order to guarantee the accessibility of the documents (specifically, for people with visual impairments), the Authority has indicated (CNS 12/2020) that, taking into account the provisions of the regulations on accessibility, it should to facilitate the option to also be able to access the same document incorporated as "image", but in textual format (FJ IV).

From here, for the purposes of being able to publish a document signed electronically, using a textual format and without the information of the certificate used to sign it being accessible, the Authority proposes, among other possibilities, the following options (FJ V):

A first option would be to assess the possibility of eliminating the properties of the certificate used in the electronic signature of the document, keeping the image generated in the signature process (which would not incorporate the DNI), without having to transform all the text of the document into an image .

Thus, in the case, for example, of pdf documents, an option to be able to delete the data of the electronic signature while preserving the image of this would be to create a new pdf document using a virtual printer to convert to pdf (option "Microsoft print to pdf" from the print menu).

This will generate a pdf document in text format, which would not require specific text recognition (OCR) technology to be able to read it.

This would, therefore, be an appropriate option in order to disseminate certain documents, making it easier for people who can consult them to read them, through screen readers.

Another option would be to certify that the document to be disseminated has been signed by a specific person, through some digital verification system that does not incorporate the data that is part of the certificate of the person signing the act, but only of the 'organ that makes the check.

This is without prejudice, of course, to the fact that the name and surname of the person who signed it must also be stated in the document, in order to exercise the right to know the identity of the person who signed the administrative act .

In this way, the recipients or those who can access the document disseminated would have the guarantee (through the aforementioned verification system) that a certain person has signed the document, but they would not be able to access the personal data (the ID number) that it is contained in the information included in the digital certificate of the person who signed it.

A technological solution such as the "eCópia" solution of the AOC would allow this check to be carried out in a way that fully respects the protection of personal data.

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

Conclusions

From the point of view of the right to data protection, it would be necessary to assess the possibility of establishing a certification policy that foresees the use of qualified public worker certificates based on pseudonyms.

In order to avoid the dissemination of the ID number in the publication of documents that incorporate an electronic signature, it is recommended to take into account the considerations made in section V of this opinion.

Barcelona, January 8, 2021