Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

File identification

Archive resolution of the previous information nos. IP 84 and 110/2019, referring to the Open Administration Consortium of Catalonia and the Waste Agency of Catalonia.

Background

1. On 19/03/2019, the Catalan Data Protection Authority received a letter from a person who made a complaint regarding the T-CAT card, on the grounds of an alleged breach of the regulation on protection of personal data. In particular, the complainant stated that, as an employee of the Waste Agency of Catalonia (hereafter, ARC), she had a T-CAT card. The complainant stated that, since the last renewal of the T-CAT card, when electronically signing documents or making transfers through EACAT or e-Notum, their first and last names and their ID number were included. In this sense, the complainant considered that the inclusion of the DNI could violate the legislation on the protection of personal data.

This complaint was assigned IP number 84/2019.

2. The Authority opened a preliminary information phase, in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat , and article 55.2 of Law 39/2015, of October 1, of the common administrative procedure of public administrations (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. On 03/25/2019, as part of this preliminary information phase, the Open Administration Consortium of Catalonia (hereafter, AOC) was required to report, among others, on
the reasons why it was necessary for the ID of the person signing to be displayed in the image generated by the certificate and in the properties of the signature.

4. On 04/10/2019, the AOC responded to the aforementioned request through a letter in which set out, among others, the following:

- That the image generated by a signature based on a digital certificate is a graphic reproduction, without legal effects, embodied on an electronic document that allows visual evidence that it has been signed electronically. The lack of legal effect of the image allows the signer to configure (if the signature program allows) whether or not a signature image appears and, if so, the format and content (such as ID) that shown in the signed document.

- That the determination of the data shown in the image of an electronic signature made with a T-CAT card does not depend on this electronic certificate, but on

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

program that the user uses to sign in and the configuration possibilities that this program supports and that the user has defined.

- That the AOC informs T-CAT users about how a PDF document can be modified so that no information about the signatory's ID appears in the image of the signature.
- That, on the other hand, the signature properties are those data contained in an electronically signed document, corresponding to the fields that make up a digital certificate (some of which are mandatory). These fields are predefined and are not editable by qualified certification service providers.
- That the standardization of the fields that must contain a type of electronic certificate allows the generated signatures to be recognised, interoperable and validated.
  The signature properties of the certificate and, therefore, the electronic signature, is one of the components of electronic documents, as well as a requirement for the validity of administrative electronic documents.
- That the AOC has no authority as a lender to decide whether or not the DNI can be viewed by accessing the signature properties of an electronic document. This issue is conditioned by the regulations that determine in a standardized way the structure (fields and contents) of an electronic certificate, which aims to ensure the recognition and interoperability of certificates.

- That in accordance with art. 2.2 of Law 59/2003, of December 19, on electronic signature (hereinafter, LSE) a certification service provider is that *"natural or legal person that issues electronic certificates or provides other services in relation to electronic signature"* . For its part, article 3.20 of 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 (hereafter ReIDAS), defines qualified providers of trust certification services as those who provide one or more qualified trust services, to which the supervisory body has granted the qualification.

- That article 11.2.e) of the LSE establishes that recognized or qualified certificates must include *"the identification of the signatory, in the case of natural persons, by their first and last name and the number of their national identity document or through a pseudonym that is clearly stated as such".*
- That as indicated by the Authority in opinion CNS 15/2013: *"[…] it can be considered that the use of the name and surname of the natural person who signs together with his ID number, in the terms raised in the consultation , has sufficient legal coverage in the LSE. The minimum content that recognized certificates must have is that set out in article 11.2 of the LSE, which includes, among others, the identification of the natural person who signs, through their first and last name and their number of ID, without this being considered contrary to the Directive."* In the same sense, the Authority pronounced in opinion CNS 17/2017.

- That any reliable certification service provider, such as the AOC, must comply with the current regulatory provisions regarding the structure of electronic certificates, which establish the obligation to include the DNI data.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

- That the General Administration of the State (hereinafter, AGE), in compliance with article 18 of Royal Decree 4/2010, of January 8, which regulates the National Interoperability Scheme (hereinafter , ENI) and of the Technical Interoperability Rule for Electronic Signature and Seal Policy and Certificates of the Administration, approved an Electronic Signature and Certificate Policy. This Policy *"will serve as a general interoperability framework for the authentication and mutual recognition of electronic signatures within its scope of action. However, said policy can be used as a reference by other public administrations to define the policies of certificates and firms to be recognized within their areas of competence" (article* 18.1 ENI).

- That article 18.4 of the ENI establishes that *"The common profiles of the certificate fields defined by the electronic signature and certificate policy will enable interoperability between user applications, so that both the identification and the electronic signature generated from these common profiles can be recognized by the applications of the different public administrations without any type of technical, semantic or organizational restriction."*

- That the aforementioned Policy is applicable in those cases where, as in Catalonia, an own electronic signature policy has not been developed.
- That in the document *"Profiles of electronic certificates"* of April 2016 , as part of its Electronic Signature and Certificates Policy, the AGE defines what the minimum fields must be for the different digital certificates, differentiating between recommended or not and fixed or optional. This is the reference document for the certificates derived from Law 40/2015, of October 1, on the legal regime of the public sector (hereafter, LRJSP).
- That with regard specifically to the public employee certificate, section 10.1 *"Criterios de composición del campo CN para un certificado de empleado público"* of the document *"Profiles de certificados electronicos"* determines what the fields and content of the fields that make up the *"Common Name" (hereinafter,* CN). Therefore, the data in the *"CN"* field is not a discretionary decision of the certification service provider, but is determined by the Ministry of Finance and Public Administrations itself (hereinafter, MHAP).

- That with regard to public employee certificates, this document determines that the data relating to the DNI is mandatory.
- That in accordance with the previous considerations, the recognized personal certificates of public workers issued by the AOC must include the DNI in the *"CN" field.*
- That the lack of inclusion of the DNI in the structure of the certificate would have direct consequences on the main functionality of the digital certificate, to the point that it would cease to be recognized as a public employee both by the AGE and by different corporate applications.
- That as the Authority recognized in its opinion CNS 17/2017, it is necessary to take into account the consequences in terms of interoperability that the non-inclusion of the DNI in the structure of qualified public employee certificates should have.
- That the issuance of certificates without following the predefined structure would lead to the loss of the condition of qualified certification service provider, the expulsion of the AOC from the trust list of qualified providers of electronic certification services *(" Trusted Service*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

*List – TSL")* and the impossibility of continuing to issue qualified public worker certificates.

- That it does not correspond to the AOC, as a provider of qualified certification services, any decision regarding the appearance of the DNI in the signature properties of an electronic document.
- That section 8 of the Resolution of 07/19/2011, of the Secretary of State for the Function Public, which approves the Electronic Document Interoperability Technical Standard (NTI-DE), which regulates access to electronic documents, establishes that *"When public administrations facilitate access to electronic documents through their electronic sites or communication channels that correspond in each case, se will show: (...) b) The basic information of each of the signatures of the document defined in Annex III."* This basic information includes the information of the document signer that must be included in the signature properties.
- That as the Authority noted in opinion CNS 17/2017, in accordance with the applicable regulations and the document *"Profiles of electronic certificates",* the DNI of the public employee on the T-CAT cards appears in the following certificate structure fields: *"SerialNumber, SurName and CommonName".*

- That in those tools that depend on the AOC, work is being done to adapt them with the aim that they do not show the DNI when viewing the signature made, thus complying with both the principle of data minimization, and privacy by default.
  This is the case, for example, of the signasuite application and the AOC signature porta.
- That the AOC has addressed on several occasions the General Secretariat of Digital Administration of the Ministry of Territorial Policy and Public Service to convey the concern generated by the fact that the qualified public worker certificates contain the DNI in the field *"CN ".*
- That the AOC offers, as an alternative to the T-CAT, the possibility of applying for public employee certificates with a pseudonym. This type of certificate anonymously preserves the identity of the signatory, as regards the information on their ID, information that is replaced in the *"CN"* of the digital certificate by a pseudonym. This alternative was already recognized by the Authority, among others, in its opinion CNS 15/2013.
- That the request and issuance of this type of certificate remains conditional on compliance with the applicable regulations, having to deal with pseudonyms that are clearly stated as such and for regulated groups of workers public

5. On 09/04/2019, the Authority received a letter from another person who indicated that she was an employee of a local body (which she did not specify), for which she made a complaint also regarding the T-CAT card. Specifically, the complainant stated that, when he signed any electronic document addressed to the administration, the image that was generated contained his ID. In turn, he added that his ID also counted in the properties of the signature. In the last one, the complainant stated that his ID number *"is personal data that should not appear in the digital subject as a public official."*

This complaint was assigned the number IP 110/2019.

Fundamentals of law

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

1. In accordance with the provisions of articles 90.1 of the LPAC and 2 of Decree 278/1993, in relation to article 5 of Law 32/2010, of October 1, of the Authority Catalan Data Protection Agency, and article 15 of Decree 48/2003, of February 20, which approves the Statute of the Catalan Data Protection Agency, the director of the Catalan Data Protection Authority.

2. Based on the account of facts that has been set out in the antecedents section, it is necessary to analyze the reported facts that are the subject of this file resolution, referring to the T-CAT card that public employees have the Generalitat de Catalunya and local administrations, which contains a recognized or qualified digital certificate.

2.1. About the image that is generated when signing a document electronically.

In this sense, the Authority has pronounced in opinions CNS 17/2017, 23/2017, 58/2018 and 1/2019, in the following terms:

> *"(...) the appearance or image of a signature based on a certificate is something that can be pre-defined a priori through the options offered in this regard by the program used to sign electronically (for example, Adobe Acrobat), so the data of the public worker that is incorporated in the electronic certificate does not necessarily have to be visible once the document has been electronically signed. The visibility or not of this personal data will depend, therefore, on the way in which the format of said signature has been pre-established. And this regardless of the type of electronic certificate that the worker has."*

So things, the appearance or image that is generated when signing an electronic document using the digital or recognized certificate (T-CAT), and in particular, the data that is displayed can be configured through the program through which it is signed .

This circumstance, as will be explained later, must entail that corrective measures are required in this respect.

2.2. On the Spanish regulations regarding the content of electronic certificates.

In this sense, the AOC invokes in its letter of response to the request made to it, that this Authority stated in the opinion CNS 15/2013 that *"it can be considered that the use of the name and surname of the natural person who signs together with his ID number, in the terms set out in the consultation, he has sufficient legal coverage in the LSE. The minimum content that recognized certificates must have is that set out in article 11.2 of the LSE, which includes, among others, the identification of the natural person who signs, through his name and*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

*surnames and their ID number, without this being considered contrary to the Directive."*

In this regard, it should be noted that this opinion predates ReIDAS, which was applicable from 01/07/2016 (Article 52.2 of ReIDAS), so with regard to the content of qualified or recognized certificates must take into account the provisions of this European regulation.

Once this point has been made, it should be borne in mind that the DNI is also accessible by anyone receiving the document electronically signed by a public employee, by consulting the properties of the signature where you can see all the information fields that are part of the structure of the certificate (among which, the DNI of the public employee is included). It is worth saying that, as stated by this Authority in opinion CNS 17/2017, this configuration cannot be modified by the public worker, nor by the Public Administration to which it belongs.

Having established the above, it is necessary to decide whether the inclusion of the data relating to the DNI of the public employee in said electronic certificate is necessary.

Firstly, sections 1 and 2.e) of article 11 of the LSE, which refer to the concept and content of recognized certificates, provide that:

> *"1. Recognized certificates are electronic certificates issued by a certification service provider that meets the requirements established by this Law regarding the verification of the identity and other circumstances of the applicant and the reliability and guarantees of the certification services they provide.*
> *2. The recognized certificates must include, at least, the following data: (...)*
> *e) The identification of the signatory, in the case of physical persons, by their first and last name and their national identity document number or through a pseudonym that is clearly stated as such and, in the case of persons legal entities, by their name or company name and their tax identification code."*

As stated in the opinion CNS 17/2017, in accordance with the precept transcribed, the identification of the signatory in the configuration of the certificate recognized by the certification service provider can be carried out *"indicating the name , surnames and ID as a pseudonym, replacing these data".*

For its part, sections 1 and 4 of article 18.1 of the ENI establish that:

> *"1. The General Administration of the State will define an electronic signature and certificate policy that will serve as a general interoperability framework for the authentication and mutual recognition of electronic signatures within its scope of action. However, said policy may be used as*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

*reference by other public administrations to define the policies of certificates and firms to be recognized within their areas of competence. (...)*
*4. The common profiles of the certificate fields defined by the electronic signature and certificate policy will enable interoperability between user applications, so that both the identification and the electronic signature generated from these common profiles can be recognized by the applications of the different public administrations without any type of technical, semantic or organizational restriction. These certificates will be those defined in Law 11/2007, of June 22, Law 59/2003, of December 19, on electronic signatures and their regulatory developments."*

As reported by the AOC by means of a letter dated 04/09/2019, the electronic signature and certificate policy approved by the General Administration of the State (hereinafter, AGE), is applicable insofar as Catalonia has not developed its own.

For its part, in the document *"Profiles of electronic certificates"* prepared by the MHAP in 2016, the content of the fields for electronic certificates of public employees (sections 5.3 and 10.1) and for electronic certificates of public employees with a pseudonym is established (sections 5.4 and 11.1).

In relation to the first (section 10.1), the composition criteria of the *"CN"* field of the certificate provide, among others:

*"• Compulsorily include the DNI/ NIE number, together with the control letter, according to what is indicated in the DNI/ NIE.*
*• Compulsorily include a SYMBOL or CHARACTER that separates the number and last name from the ID number."*

In turn, section 10.2 of the aforementioned document also provides for the inclusion of the DNI number as mandatory in the *"Surname"* field of the certificate (field 1.5.9) and as recommended in the *"SerialNumber"* field (field 1.5 .8).

In accordance with the above, in the *"CN"* and *"Surname"* fields that are part of the structure of the electronic certificate of public employees, the inclusion of the ID number is foreseen as mandatory. And in the *"SerialNumber" field,* the inclusion of this data is optional.

And with regard to the electronic certificates of public employees with a pseudonym (section 11.1), it is expressly provided that in the *"CN" field "The DNI/ NIE number may not be included".* It is worth saying that the aforementioned document also restricts the use of these certificates with pseudonyms by public employees to the cases contemplated in RD 1671/2009.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

In short, in accordance with the regulations set out in this section (and in particular article 11.2 of the LSE), the minimum content of the recognized or qualified certificates could include the data relating to the DNI.

2.3. About the *"ETSI EN 319 412-2" standard.*

Having established the above, it is necessary to mention the standard *"ETSI EN 319 412-2" "Certificate profile for certificates issued to natural persons"* which, precisely, supports the requirements of the qualified certificates required in the ReIDAS, and which also refers to 'mentioned document of the MHAP to specify the information that must be included in the qualified public worker certificates. In this regard, the following was pointed out in CNS opinion 17/2017:

> *"According to this rule, the field relating to the signatory (Subject) of the certificate must include the attributes: country (CountryName), name and surname or pseudonym of the signatory (GivenName and Surname or Pseudonym), and CN.*
>
> *The inclusion in the certificate of the attribute relating to a number or identification code of the signatory (SerialNumber), as would be the case of the DNI, is considered pertinent only in those cases in which the establishment of the previous attributes ( CountryName, GivenName and Surname or Pseudonym, and CN) the signatory cannot be unequivocally identified. Add the rule that this SerialNumber field has no defined semantics (it does not specify what information could be included), so it could be a number or a code assigned by the certification body (the AOC Consortium) or an identification number assigned by the national State (the DNI or the worker's professional identification code, for example).*
>
> *Likewise, the rule provides that the CN field must contain a name of the person signing and that it is allowed to do so in different formats or even the use of pseudonyms and aliases, given that, unlike the GivenName and SurName or Pseudonym field , this is a field that is used to provide information about the identity of the person signing informally."*

In accordance with this rule, the inclusion of the DNI data in the *"CN"* field of the qualified certificates of public workers would not be relevant or necessary, for the purposes of identifying the person signing, given that this identification would be achieved with the name and surnames of the public employee, as it happens in documents signed by hand.

Likewise, it should be borne in mind that the possible risk of two people having the same first and last name is avoided with other information that is also contained in the qualified certificate, such as the name of the entity where the employee provides services - field *"Organization"-;* as well as the predictable inclusion of the charge in the signature footer.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

Also in relation to the identification of the signatory, article 24.1 of ReIDAS establishes that qualified providers of trust services (such as the AOC) must comply with the following requirements:

> *"1. When issuing a qualified certificate for a trust service, a qualified trust service provider will verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attribute of the natural or legal person in the that a qualified certificate is issued.*
>
> *The information referred to in the first paragraph will be verified by the trusted service provider either directly or through a third party in accordance with national law: a) in the presence of the natural person or an authorized representative of the person legal entity, or) remotely, using means of electronic identification, for which the presence of the natural person or an authorized representative of the legal entity has been guaranteed prior to the issuance of the qualified certificate, and which meet the requirements established with the article 8 with respect to the "substantial" or "high" security levels, or) by means of a certificate of a qualified electronic signature or a qualified electronic seal issued in accordance with letter a) or), or) using other nationally recognized identification methods that provide equivalent security in terms of reliability to physical presence.*
>
> *Equivalent security will be confirmed by a conformity assessment body."*

In accordance with the precept transcribed, it must be taken into account that the identity of the public employee holding the qualified certificate is already verified when it is issued.

In the same sense, and with regard to the use of pseudonyms, article 17.3 of the LSE establishes that *"providers of certification services who record a pseudonym in the electronic certificate at the request of the signatory must verify the his true identity and keep the documentation that proves it."*

2.4. On European regulations regarding the content of electronic certificates.

At this point, it is appropriate to refer to the forecasts contained in the ReIDAS.

As pointed out in CNS opinion 17/2017, article 50 of the ReIDAS repealed *"the Directive 1999/93/EC of the European Parliament and of the Council, of December 13, 1999, which establishes a community framework for electronic signatures, which Spain transposed with the aforementioned LSE, so it is necessary to have given that the entry into force of this ReIDAS,*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

*of direct application in each Member State from July 1, 2016 (article 52), it would leave without effect those precepts of the LSE that oppose it."*

Having made this point, article 51.2 of ReIDAS provides as transitional measures that *"Recognized certificates issued for natural persons in accordance with Directive 1999/93/EC shall be considered qualified electronic signature certificates in accordance with this Regulation until they expire. "*

So things are, once the certificates issued prior to ReIDAS expire, the new certificates that are issued must conform to the provisions of this European standard.

In this sense, sections 1 to 3 of article 28 of ReIDAS provide that:

> *"1. Qualified electronic signature certificates will meet the requirements established in Annex I.*
> *2. Qualified electronic signature certificates will not be subject to any mandatory requirement that exceeds the requirements established in Annex I.*
>
> *3. Qualified electronic signature certificates may include additional non-mandatory specific attributes. These attributes will not affect the interoperability and recognition of qualified electronic signatures."*

And Annex I, to which sections 1 and 2 of the transcribed precept are referred to, establishes the requirements for qualified electronic signature certificates, which includes what is provided for in letter "c":

> *"c) at least the number of the signatory or a pseudonym; if a pseudonym will be used, it will be clearly indicated;*

Therefore, ReIDAS only requires that the qualified certificate contain the name of its holder or a pseudonym. On the contrary, as explained, the LSE (Article 11.2.e) requires the ID number to be included as well, unless a pseudonym is used.

In relation to the above, the Authority pronounced in opinion CNS 17/2017 in the following terms:

> *"Considering that the Regulations are mandatory in all their elements and directly applicable to the Member States (Article 288 TFEU), it should be considered whether the internal rule (LSE) can establish or foresee more requirements when identifying the person signing that those established, in this case, in the ReIDAS.*
>
> *In this regard, it is appropriate to agree that it is consolidated jurisprudence of the Court of Justice of the European Union (among others, judgment of October 14, 2004, case c113/02, judgment of December 21, 2011, case c-316/10,*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

*or judgment of October 25, 2012, case c-592/11) that Member States may adopt measures to implement a Regulation as long as these do not hinder their direct applicability, do not hide their community nature and regulate the exercise of the margin of appreciation that the Regulation in question gives them, staying in any case within the limits of its provisions.*

*That is to say, the fact that EU regulations appear in a Regulation (as in this case) does not necessarily mean that any national measure to implement these regulations is prohibited. Moreover, the CJEU admits that, although, due to the nature of the Regulation, its provisions have an immediate effect on national legal systems, some provisions of the Regulations may require, for their execution, the adoption of measures of application by the Member States. It is necessary, in the words of the Court, to refer to the specific provisions of each Regulation to check whether these, interpreted in accordance with the objectives of said Regulation, prohibit, require or allow the Member States to adopt certain enforcement measures and, in particular in the latter case, if the measure falls within the margin of appreciation recognized in all Member States."*

As advanced, Annex I of ReIDAS only requires, as a minimum content of qualified certificates, the inclusion of the signatory's name (or a pseudonym), for the purposes of enabling their identity. As pointed out in opinion CNS 17/2017, *"this provision, which would facilitate the interoperability of electronic signatures between Member States, seems reasonable, given that in many EU countries citizens are not required to have a personal identification document, such as the DNI in the case of Spanish citizens over the age of 14 (Royal Decree 1553/2005, of 23 December, which regulates the issuance of the DNI and its electronic signature certificates )."*

And it was added that *"The requirement to include the DNI in the certificates, referred to by the LSE, could only be understood as valid, with regard to ReIDAS, to the extent that this data was incorporated as an additional specific attribute not mandatory and as long as doing so would not compromise the interoperability and recognition of the qualified electronic signature. Otherwise, the forecasts of the LSE would be displaced by what is established in the ReIDAS."*

2.5. About interoperability.

In its written response to the request made by this Authority, the AOC invoked that the regulations that determine in a standardized way the structure (fields and contents) of an electronic certificate, aim to ensure the recognition and interoperability of certificates And he added that the lack of inclusion of the DNI in the structure of the certificate would have direct consequences on the main functionality of the digital certificate, to the point that

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

he would no longer be recognized as a public employee both by the AGE and by different corporate applications.

In this regard, it should be emphasized again that in accordance with the ReIDAS, to which the electronic certificate of public employees is subject, the inclusion of the DNI (annex I) would not be mandatory, but in any case the assignment of any other information ( as could be the case with the DNI) would remain limited to the fact that this assignment was not mandatory (Article 28.2 of ReIDAS) and to the fact that the interoperability of the qualified signature was not compromised (Article 28.3 of ReIDAS).

In other words, the lack of ID cannot affect interoperability. On the other hand, its inclusion in the digital certificate can actually harm it.

At this point, as stated in recital 54 of the ReIDAS, *"Interoperability and cross-border recognition of qualified certificates is a prerequisite for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates must not be subject to any mandatory requirement that exceeds the requirements established in this Regulation. However, at the national level, the inclusion of specific attributes, for example unique identifiers, in qualified certificates must be allowed, provided that such specific attributes do not compromise the cross-border interoperability and recognition of certificates and qualified electronic signatures."*

So things are, in the present case interoperability must not only be guaranteed at state level, but in all the Member States of the European Union. In turn, recital 54 of ReIDAS states that the inclusion of other specific attributes in qualified certificates cannot compromise interoperability, the cross-border recognition of certificates and qualified electronic signatures. And, in this sense, it is true that the said recital refers to the possibility that unique identifiers can be included at national level, but these do not necessarily have to be the DNI. Indeed, these unique identifiers can be any pseudonymized data linked to the person holding the certificate.

In turn, as has already been explained, the *"ETSI EN 319 412-2" standard* also does not require the inclusion of the DNI to guarantee interoperability at Community level.

On the other hand, in the opinion CNS 17/2017 it was also analyzed that the inclusion of the DNI data could respond to the need to guarantee interoperability between user applications.

Certainly, article 18.4 of the ENI provides that the common profiles of the certificate fields defined by the electronic signature and certificate policy will enable interoperability between user applications, so that both the identification and the electronic signature generated from of the common profiles of the certificate fields can be recognized by the applications of the different Public Administrations without any type of technical, semantic or organizational restriction.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

However, as pointed out in the aforementioned opinion, if this is the purpose pursued, it does not seem that including the DNI data in the *"CN"* field of the certificate is the most appropriate option, given the cases that usually occur in the allocation of information to this type of certificate, benefiting from the large volume of certificates to be issued (large volume of public workers) and the diversity of certification service providers that can issue them. The MHAP document itself refers to these circumstances.

2.6. On the principle of minimization.

Article 5.1.c) of Regulation (EU) 2016/679 of the Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of 'these data and which repeals Directive 95/46/CE (hereinafter, RGPD), contemplates the principle of minimization as one of the principles relating to the processing of personal data. According to this principle, personal data will be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".*

Likewise, Recital 39 of the RGPD states that *"Personal data should only be processed if the purpose of the treatment cannot reasonably be achieved by other means."*

In accordance with this principle of minimization, the data of public workers included in the configuration of electronic signature certificates must be the minimum necessary to fulfill the intended purpose.

In this way, if the purpose pursued in a certain context can be achieved without the need to carry out the processing of a certain data, without this purpose being altered or harmed, this possibility should necessarily be chosen , given that the processing of personal data implies, as enshrined by the Constitutional Court in Sentence no. 292/2000, a limitation of the right of the affected person to dispose of the information referred to his person.

For its part, article 5 of ReIDAS regarding the treatment and protection of data, provides the following:

> *"1. Personal data will be processed in accordance with Directive 95/46/ EC.*
>
> *2. Without prejudice to the legal effects that national legislation provides for pseudonyms, their use in electronic transactions will not be prohibited."*

The referral of ReIDAS to Directive (EU) 95/46/EC, must be understood as carried out in the RGPD as established in article 94.2 of the RGPD.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

Well, as specified by the Authority in opinion CNS 17/2017, *"This identification of the public worker, by application of the principle of minimization, should occur in the same way as if the action was not carried out by electronic media In other words, only your first and last name should be provided, information that could be completed with the indication of your position or workplace and the Administration to which it belongs."*

Therefore, the public employee does not have the duty to bear the fact that the data relating to his ID is revealed, either through the appearance or image that is generated when signing electronically, nor through the consultation of the properties of the signature of the qualified or recognized certificate.

Having said that, article 53.1.b) of the LPAC recognizes the right of interested parties to *"identify the authorities and staff at the service of the public administrations under whose responsibility the procedures are processed."*

As indicated by the Authority in opinion CNS 17/2017, *"Regarding the identification of the public worker who signs a certain administrative document, 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 served him in his performance before the Public Administration. Knowing the DNI of the public worker, in fact, would not contribute or improve the identification of the worker, given that the citizen does not have the appropriate means to check the veracity of this personal information."* And it was added that this *"action by public workers (signing the relevant documents) transferred to the field of electronic administration must not detract from their fundamental right to the protection of personal data (Article 18.4 EC) ."*

In short, in accordance with everything that has been set out in this resolution, it must be concluded that it is not necessary to include the DNI in the qualified certificates of public employees, nor for their identification (in particular, before the public) , nor to guarantee interoperability.

Indeed, as already indicated in CNS opinion 17/2017, ReIDAS does not prevent the issuance of qualified electronic signature certificates with a pseudonym, that is, certificates that do not contain personal identifying data (name, surname or DNI) of the person signing. And it was added that *"The certification service provider will be the one who has the information that links a qualified certificate to a specific person. The use of pseudonyms, therefore, is an equally valid option for the purposes of establishing the identity of the person signing, without this diminishing the use, capacity or functionality of qualified certificates."*

In turn, Article 5.2 of ReIDAS already provides that Member States cannot prohibit the use of pseudonyms in electronic transactions.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

Therefore, nothing prevents that in the fields that make up the digital certificate that contain the DNI of public employees (CN, Surname and SerialNumber), this data is replaced by a unique pseudonym assigned by the AOC or by the Administration or entity where the employee provides services.

At the same time, the use of pseudonyms in the indicated fields also guarantees the interoperability of the qualified certificate, taking into account that the replaced data (the DNI) is not necessary in accordance with the requirements of qualified electronic signature certificates required by ReIDAS (annex I) and that the LSE itself supports its use (art. 11.2.e) without restricting it to any specific case.

In short, from the perspective of the principle of data minimization, the inclusion of the DNI in the qualified or recognized certificates is inadequate data, not relevant and not limited to what is necessary for its use.

2.7. About data protection in design.

Having arrived at this point, it should be made clear that one of the obligations imposed by the RGPD (Article 25.1) on data controllers is the protection of data in the design:

> *"1. Taking into account the state of the art, the cost of the application and the nature, scope, context and purposes of the treatment, as well as the risks of varying probability and seriousness that the treatment entails for the rights and freedoms of people physical, the person in charge of the treatment will apply, both at the time of determining the means of treatment and at the time of the treatment itself, appropriate technical and organizational measures, such as pseudonymization, designed to effectively apply the principles of data protection, as the minimization of data, and to integrate the necessary guarantees in the treatment, in order to fulfill the requirements of this Regulation and protect the rights of those interested."*

Therefore, the data controller must implement the appropriate technical and organizational measures to implement data protection principles. As indicated in Recital 78 of the RGPD *"Such measures could consist, among others, of reducing the processing of personal data to the maximum, pseudonymizing personal data as soon as possible, giving transparency to the functions and the processing of personal data, allowing to those interested in supervising data processing and to the data controller to create and improve security elements. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or that process personal data to fulfill their function, the producers of the products, services and applications should be encouraged to take into account the right to data protection when they develop and design these products, services and applications, and to ensure, with due attention to the state of the art, that those responsible and those in charge of treatment are in a position to fulfill their obligations in matter of protection of*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

*data The principles of data protection by design and by default must also be taken into account in the context of public contracts."*

Data protection by design must be implemented both at the time of determining the means of treatment, as well as once treatment has begun. In the latter case, the controller continues to have the obligation to implement the principles relating to treatment and, as far as is concerned, to periodically analyze whether the personal data that is the subject of treatment is still adequate, relevant and limited.

2.8. About pseudonyms.

In opinion CNS 17/2017, this Authority already analyzed the possibility of using pseudonyms in a generalized way in the qualified certificates of public employees. Specifically, it stated the following:

> *"This possibility, although it could be conflicting in view of the provisions of 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 declaration of certification practices and therefore define the profiles of the certificates it issues (article 19 LSE).*
>
> *Therefore, the AOC Consortium could establish, in the public worker qualified certificate profile, that the identification of the person signing will be carried out, in general, through a pseudonym. This pseudonym could be the first and last name of the public worker and, where appropriate, position or category, provided that, for reasons of public security, it is not required to preserve their anonymity.*
> *In 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.*
>
> *In the event that, certainly, for reasons of public security, the anonymity of the public worker should be guaranteed, the pseudonym could be his professional identification code, insofar as this is not related to personal data of the public worker (such as the ID number), or any other indicator provided by the Public Administration in which it provides its services.*
>
> *In both cases it should be clearly indicated that it is a pseudonym (annex I ReIDAS)."*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

So things are, taking into account the principle of data minimization (art. 5.1.c RGPD) and the obligation to guarantee data protection in the design (art. 25.1 RGPD), the AOC must adopt the appropriate measures so that the qualified certificates issued to public employees do not include their ID, such as those just transcribed.

In this sense, it should be noted that these measures cannot be restricted only to the cases provided for by the MHAP (classified information, public security, national defense or other actions in which anonymity is legally justified), which are governed by its specific regulations as provided in article 4.4 of the LSE.

Therefore, they must apply to all public employees.

2.9. About the responsibility of the AOC.

In the present case, it should be borne in mind that, for the issuance of qualified certificates to public employees, the AOC followed the parameters established by the MHAP, which provide for the inclusion of the DNI in the certificates.

The above could give rise to the interpretation that, in accordance with the said instructions of the MHAP, the general rule was that in the certificates issued to public employees the DNI had to be included and that the use of a pseudonym was only reserved to specific cases.

For these reasons, it has been considered that the AOC would have acted with the conviction that it did not commit any infringement of the regulations on data protection by including the DNI of public employees in the qualified certificate, for the purposes of guaranteeing its recognition and its interoperability

Therefore, by application of the principle of responsibility or culpability (art. 28 LRJSP), it is not appropriate to initiate a sanctioning procedure, as in this specific case, it may be excessive to invoke the entity's lack of diligence.

All this, without prejudice to the warning and the corrective measures that will be required later, to avoid the disclosure of the DNI of its employees as a result of the use of qualified certificates.

2.10. About the responsibility of the ARC and a local entity.

For their part, the ARC and the local entity where the second reporting person provides services (of which there is no record and which was not the subject of the report), would be responsible for implementing the appropriate measures to modify the aspect or the signature image of your public employees based on a qualified certificate, in order to ensure that the ID cannot be viewed. Is in

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

say, to create a new aspect of the signature that incorporated only the data relating to the first and last name and position, through the software used for the electronic signature.

However, it cannot be attributed to these entities that in the qualified certificate of public employees issued by an entity providing qualified certification services (the AOC), the DNI of its holder is incorporated.

In turn, if this data had not been incorporated into the certificate, the image or appearance that is generated when signing electronically would in no case include the DNI. At this point, reference should be made to what has been explained in the previous section regarding the provisions of the Spanish regulations and the indications of the MHAP regarding the inclusion of the DNI in digital certificates.

Well, all of the circumstances indicated also lead to the conclusion that it is not appropriate to initiate a sanctioning procedure against these entities, in application of the principle of responsibility or guilt.

All this, without prejudice to the warning and the corrective measures that will be required later, to avoid the disclosure of the DNI of its employees as a result of the use of qualified certificates.

3. In accordance with everything that has been set out in sections 2.9 and 2.10 of the 2nd legal basis, it is necessary to agree on its archive.

4. Article 58.2.a) of the RGPD empowers the control authorities, in the exercise of their corrective powers, in order to issue a warning to the person in charge, if the planned processing operations may infringe the provisions of the RGPD . In turn, article 8.2.c) of Law 32/2010 empowers the director of the Authority to require those responsible and those in charge of the treatment to adopt the necessary measures for the adequacy of the treatment of personal data subject to investigation in current legislation.

It is by virtue of this faculty that, despite the filing decision based on the arguments expressed in section 2.9 and 2.10 of the 2nd legal foundations, on the one hand, both the AOC and the ARC, that the treatment of the DNI of public employees in the framework of the configuration or use of qualified or recognized certificates, infringes the regulations on data protection.

And on the other hand, it is also considered appropriate to make the following requirements.

4.1. On the one hand, the AOC should be required to take the relevant actions to avoid that the qualified certificates issued to public employees do not include their ID, such as those set out in this resolution.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

4.2. On the other hand, it should be recommended to the ARC that, while the AOC does not implement the previous measure corrector, carry out the following actions:

4.2.1. Modify the appearance or image of the signature of your employees made through a qualified certificate, so that your ID does not appear there. For example, the ARC can define in the program used to sign electronically, the data that is visible once a document has been electronically signed.

4.2.2. In relation to all electronic documents addressed to other bodies or individuals signed by your employees using a qualified certificate, send only to its recipients an authentic copy of the original (this action prevents the ID of the signatory from being viewed).

It is worth saying that in accordance with article 27.2 of the LPAC, authentic copies have the same validity and effectiveness as the original documents.

This, without prejudice to other measures such as using an organ seal.

And, with regard to the publication of electronic documents, aside from the actions already indicated, as pointed out in the CNS opinion 1/2019, they could also publish electronic documents without incorporating signatures; or, convert the document to be published to "image" format, which would not allow access to the signature properties.

Given that the local body where the second complainant provides services is unknown, who addressed his letter of complaint against the entity he considered to be the provider of qualified certification services, no request can be made in this regard.

resolution

Therefore, I resolve:

1. File the previous information actions numbers IP 84/2019 and IP 110/2019, relating to the Open Administration Consortium of Catalonia (IP 84/2019 and IP 110/2019) and the Waste Agency of Catalonia (IP 84/2019).

2. Warn the AOC and the ARC that, in the event that they do not implement the measures indicated in the 4th legal basis, the processing operations that have been addressed in this resolution could infringe the provisions of the protection regulations of data

3. Notify this resolution to the AOC, the ARC and the two complainants.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

4. Order the publication of the resolution on the Authority's website (www.apd.cat), in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with article 14.3 of Decree 48/2003, of 20 February, which approves the Statute of the Catalan Data Protection Agency, the persons interested parties may file, as an option, an appeal for reinstatement before the director of the Catalan Data Protection Authority, within one month from the day after their notification, in accordance with what provided for in article 123 et seq. of Law 39/2015. An administrative contentious appeal can also be filed directly before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998 , of July 13, governing the contentious administrative jurisdiction.

Likewise, interested parties may file any other appeal they deem appropriate to defend their interests.

The director,