

CNS 12/2020

Opinion in relation to the consultation of a University on the measures to be taken to reconcile compliance with the legislation on accessibility with the regulations on the protection of personal data, in relation to the documents with digital or electronic signature that are published in the electronic headquarters

A letter from a Catalan University is presented to the Catalan Data Protection Authority, in which it is stated that it converts digitally signed documents, which are made public on its electronic headquarters, into an image, to prevent the access to the DNI number that appears in the properties of the electronic certificate of the signatories.

The consultation adds that this measure does not allow people with visual impairments to be able to access information about the digital signatures of the documents or the content of the documents themselves, since the document as an image is not suitable for keyboards or specific programs replica

For this reason, the University requests a report in relation to the possible measures to be taken to reconcile compliance with the legislation on accessibility with the regulations for the protection of personal data.

The request, which is not accompanied by more information, has been analyzed, in view of the current applicable regulations, in view of the report of the Technology and Information Security Area of the Catalan Data Protection Authority, and the report of the 'Legal Advice, the following is ruled.

I

(...)

II

The consultation explains that the University has disseminated the necessary protocols to avoid the processing and dissemination of unnecessary or excessive personal data, among others, in documents with digital or electronic signatures, in compliance with data protection regulations.

According to the inquiry, the University converts the digitally signed documents, which are made public on its electronic website, into an image, to prevent access to the DNI number of the signatories, taking into account data protection regulations.

The consultation adds that this measure, which guarantees compliance with the principle of minimization in the processing of personal data, means that people with visual impairments cannot access the information on the digital signatures of the documents or the content of the documents themselves, since document as an image is not suitable for keyboards or specific mirroring programs.

According to the consultation, this does not allow adequate compliance with the requirements of the legislation on accessibility for people with disabilities (in case of visual impairment), as required by the applicable regulations.

With the consultation in these terms, it is necessary to start from the basis that, according to article 4.1) of Regulation (EU) 2016/679, of April 27, general data protection (RGPD), they are personal data. any information about an identified or identifiable natural person ("the interested party"); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a number, an identification number, location data, an online identifier or one or more elements of identity, shall be considered an identifiable physical person physical, physiological, genetic, psychological, economic, cultural or social of said person;

Therefore, it is personal information subject to the principles and guarantees of the data protection regulations (RGPD and Organic Law 3/2018, of December 5, Protection of personal data and guarantee of digital rights (LOPDGDD)), all that information referring to identified or identifiable natural persons who may be the subject of treatment by the University, in particular, through publication on the University's electronic headquarters.

III

At the outset, it should be noted that the query refers to the dissemination by the University, through its electronic Headquarters, of digitally signed documents, without further details. The applicable regulatory framework provides that Universities, in different areas (recruitment, financial management of the University, teaching or university research projects, etc.), must disseminate various documentation.

The general regulations on transparency must be taken into account, specifically Law 19/2013, of December 9, on transparency, access to public information and good governance (LT), as well as Law 19/2014, of December 29 December, on transparency, access to public information and good governance (LTC), legislation that is applicable to public universities (art. 2.1.d) LT and art. 3.1.c) LTC).

Public Universities, as is the case of the one formulating the consultation, must comply with the requirements of the transparency legislation and provide certain information in relation, among others, to the institutional organization and the administrative structure (art. 9 LTC), or with economic, accounting, budgetary and patrimonial management (art. 11 LTC).

Given that the query refers, without further details, to documentation published on the University's website, it should be taken into account that there may be documentation that, where appropriate, may be published indicating only the first and last name or the position that the person who it is signed, or by the responsible body, without the need to include the signature of these persons. In these cases, it does not seem that the problem raised by the query should be presented.

As the query points out, this Authority has analyzed the processing of personal data following the publication of documents that incorporate an electronic signature, specifically, with regard to the incorporation of the DNI number in the electronic signature, from the perspective of the principle of minimization, according to which the data that is the subject of treatment must be adequate, relevant and limited to what is necessary in relation to the purpose of the treatment (art. 5.1.c) RGPD).

As has been done, among others, in Opinions CNS 17/2017, CNS 23/2017, CNS 58/2018 or CNS 1/2019, when a certain document is signed electronically using the public worker certificate issued by a certification body, there is certain personal information of this worker (in the case we are dealing with, University workers), which is accessible to those people who have access to said document (name, surname, ID number and position of the worker, among other information).

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 accessing the properties of the certificate used to sign, allows access to some unnecessary data, such as that relating to the no. ID of the person signing.

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 personnel at the service of the public administrations under whose responsibility certain procedures are processed or disseminate certain documents (article 53.1.b) LPACAP), this Authority considers it justified that the name and surname of the person signing it may appear in the document, but not their number. of ID From the perspective of the principle of minimization (art. 5.1.c) RGPD), to achieve this purpose, it would be sufficient to provide the name, surname and position, without disseminating the ID number of the person signing.

Considering this, and aside from eliminating the no. of ID of the signature that appears printed on the electronically signed document, the Authority proposed in Opinion 1/2019, cited (FJ V), different options to avoid access to the no. ID that appears in the properties of the electronic certificate with which the document was signed.

Alternatively, the following was considered:

"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 person signing, only the name, surname and position For this purpose, it would be necessary:

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

It should be borne in mind that 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 are incorporated in the electronic certificate do 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.

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 the Council, of 23 July 2014, relating to electronic identification

and trust services

for electronic transactions in the internal market, the name, surname and DNI data of the worker are incorporated together in the Common Name field of the certificate - so, if this field is shown 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 were incorporated.

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

It should be kept in mind that changing the appearance or format of the signature image does not actually prevent "access" to the signer's personal information that is included in the configuration of their public worker certificate. This information - which could only be modified by the certification service provider - is accessible through the consultation of the signature properties. However, 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 removed."

In relation to this issue, reference must be made to the tools that allow people with disabilities to be able to carry out tasks that would not be possible for them by regular means, called Assistive Technology. Specifically, it is necessary to refer, for the purposes of this opinion, to screen readers.

A screen reader makes the text contained in a document accessible, therefore, if the document complies with the requirements of the regulations (that is, following the guidelines of the consulted standard ((UNE-EN 301549:2019) , that, images containing text have a textual alternative or alternative text), this type of readers could read the document.

In this regard, it should be noted that the most used screen readers ("JAWS (Job Access With Speech)", "NVDA (Non Visual Desktop Access)", "VoiceOver - FineReader OCR Pro", "KNFB Reader", etc., have the OCR ("Optical Character Recognition") function that allows the reading of documents in image format.

However, it cannot be overlooked that, although the technologies most used as screen readers have OCR, the fact that the documents referred to in the query are non-textual images, adds another degree of difficulty to the visually impaired people when using them (who should check that the non-textual image is indeed read, installing the components of the screen reader chosen, which are necessary for this purpose, and would be conditioned by the degree of recognition that each OCR can do).

As has been verified for the purposes of this opinion, a document converted into an image can offer practical reading difficulties. For this reason, it is worth analyzing other possibilities as well.

IV

As pointed out in the consultation, it is necessary to take into account the provisions of the regulations on accessibility, specifically for people with visual impairments.

At the outset, article 5.4 of the LT provides that: "The information subject to transparency obligations will be published on the corresponding electronic sites or web pages and in a clear, structured and understandable way for those interested and, preferably, in reusable formats. Adequate mechanisms will be established to facilitate accessibility, interoperability, quality and reuse of published information as well as its identification and location."

Section 5 of the same article 5 of the LT provides that: "All information will be comprehensible, easily accessible and free of charge and will be available to persons with disabilities in a modality provided by media or in appropriate formats so that they result accessible and understandable, in accordance with the principle of universal accessibility and design for all."

Article 5.6 of the LTC provides that: "6. The Transparency Portal and the portals that are eventually created in accordance with the provisions of section 5 must be configured as an electronic platform for active advertising on the internet, must be easily identifiable and must contain the link of the electronic headquarters of the public administrations or corresponding entities. They must also comply with the recommendations of the Web Accessibility Initiative to facilitate access for people with disabilities."

According to article 5 of Royal Legislative Decree 1/2013, of November 29, which approves the revised text of the General Law on the rights of people with disabilities and their social inclusion, the specific measures to guarantee, among others, "universal accessibility (art. 2.k) of RDL 1/2013), must be applied, among others, to the field of communications and information society (art. 24 RDL 1/2013).

Article 33.4 of Catalan Law 13/2014, of 30 October, on accessibility, provides that: "Public administrations and public service providers must make accessible the information they provide via the Internet. Web pages must meet, at a minimum, the level of accessibility that is determined and must contain information about that level and the date on which the accessibility conditions were last revised. Advances and new systems that promote accessibility in communication must be gradually incorporated into the information and communication technologies that are used."

Article 5 of Royal Decree 1112/2018, of September 7, on accessibility of websites and applications for mobile devices in the public sector (transposing Directive (EU) 2016/2102, of October 26, 2016) , and which is applicable to the case at hand (art. 2.1.d) of the same R. decree and art. 2.2.c) Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations (LPACAP)), has the following:

"1. The websites and applications for mobile devices of the obliged entities included in the scope of application of this Royal Decree must be accessible to their users and, in particular, to the elderly and disabled, so that their contents are perceptible , operable, comprehensible and robust taking into account the rules of article 6.

2. Accessibility will be considered integrally in the process of design, management, maintenance and content updating of websites and applications for mobile devices.

3. The obliged entities will adopt, whenever possible, measures to increase the accessibility of their websites and applications for mobile devices with respect to the minimum level of accessibility that must be met at all times."

Article 6.3 of RD 1112/2018 referring to the presumption of compliance with accessibility requirements, provides that: "In the event that the references of the harmonized standards referred to in section 1 have not been published, it will be presumed that the content of the websites that meets the relevant requirements of EN 301 549 V1.1.2 (2015-04) or parts of them, complies with the accessibility requirements established in article 5 that are covered by said requirements or parts of them.(...)"

The European standard EN 301 549 "Accessibility requirements for ICT products and services applicable to public procurement in Europe" was approved in 2014 by the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standardization. This standard was adopted in Spain as UNE-EN 301 549 by the Spanish Association for Standardization and Certification (AENOR), the entity responsible for the development of technical standards in Spain.

The latest version of the standard EN 301 549, v.2.1.2 (UNE-EN 301549:2019, as the official version in Spanish), was published in 2018. It establishes a series of requirements for documents that are not pages web ("non-web document"), such as word documents, pdf, etc., as could be the documents referred to in the query, in relation to which it is expected that compliance with Guideline 1.1.1 of the WCAG Guidelines 2.1, referring to "non-textual content", according to which: "All non-textual content that is presented to the user has a textual alternative that fulfills the same purpose", except in certain cases that list the same guideline

As provided in these guidelines, images that contain text must have a textual alternative or alternative text. The textual alternative can be defined as a description in text format that fulfills a function as equivalent as possible to that of those elements it is describing. For example, if it is an image that contains text, the textual alternative must be the text contained in the image. Therefore, the option to be able to access the same document incorporated as an image, but in textual format, should be facilitated.

To check if alternative text is available, some programs, such as the Adobe Acrobat program, have a function to check the accessibility of a document, in this case PDF, which, among other things, generates a report with errors when the document contains images without alt text.

Therefore, initially, in those cases where the University incorporates a textual alternative, parallel to the published image, this option would not pose problems from the point of view of accessibility.

v

For the purposes of being able to publish a document signed electronically, using a textual format and without the information of the certificate that was used to sign it being accessible, there would be different possibilities. Below we list two:

A) Firstly, the University could 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 the whole document text in image.

Thus, and continuing with the example of pdf documents, an option to be able to delete the data of the electronic signature while preserving the image of it, 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 a suitable option in order to disseminate certain documents on the University's electronic headquarters, making it easier for people who can consult them to read them, through screen readers.

B) Secondly, another option would be for the University to certify that the document has been signed by a specific person, through some digital certificate system that does not incorporate the data that is part of the properties of the person's certificate that signs the act, but only of the body that performs the verification.¹ This is without prejudice, of course, to the fact that the document must also include the name and surname of the person who signed it, for the purposes of enforce 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 on the University's electronic headquarters, 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 data personal data (the ID number) 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 Consortium 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 in this opinion in relation to the query raised, the following are made,

Conclusions

Although the most used screen readers on the market have OCR, given the reading difficulties presented by documents that incorporate non-textual images, the University could choose to publish textual documents by using a virtual conversion printer to pdf.

Another option would be to use some digital verification system that the University can use, by means of a certificate that does not incorporate any physical person's data.

Barcelona, May 15, 2020

¹ This version of Opinion 12/2020 incorporates the correction of errors made on November 12, 2020.