Ref.: CNS 59/2021

Opinion in relation to the query made by the data protection representative of a City Council on the security and legal validity of a video identification system for administrative procedures

A query is presented to the Catalan Data Protection Authority by the data protection delegate of a City Council regarding the security and legal validity of a video call identification system in administrative procedures.

The data protection delegate explains that they are carrying out a pilot test of a video attention system, in which "a user accesses a video call environment controlled by the City Council on its own server, by means of a prior appointment . Once the appointment is activated, the citizen connects to the video session, first of all a message is read out loud in which the authorization for the image recording is collected. In the second term, their authentication is requested, their DNI or relevant identity document is shown, on both sides. Once the identity has been verified, by checking the data and the photograph shown, the procedure begins. Attaching documentation and receiving documentation is done in an internal cloud and integrated into the video conferencing platform, which connects to our cloud.

It is also worth saying that the recordings are all saved, including the authorization, and are linked (or will be linked, it is planned when the pilot test ends) with the file that is generated. Citizen care managers are those who attend to the person and register the documentation they provide in the corresponding procedure, in the general register."

In this context, the DPD raises the question of "whether this system can reliably guarantee the identity of the applicant, as it would be done in person or by means of a digital signature in the e-headquarters. A priori it seems that there are sufficient legal guarantees, both for the checking system and for the storage of the same in a secure environment, as indicated by the parameters of the National Security Scheme. It is also necessary to indicate that the attention systems that are foreseen, are made following the example and requirements of Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for to the issuance of qualified electronic certificates".

Having analyzed the query that is not accompanied by other documentation, and in accordance with the report of the Legal Counsel I issue the following opinion:

I

(...)

II

The data protection delegate of a City Council requests an opinion from this Authority on the security and legal validity of a citizen identification system for carrying out administrative procedures through video calls.

It is worth saying that this Authority does not have any other information about the video call identification system beyond the summary about its operation that is made in the consultation, collected in the antecedents of this opinion.

As indicated, users access a video call environment controlled by the city council on its own server by appointment (it is not indicated which identification system is used to request this appointment prior nor the procedures that can be carried out through this channel, although there is talk of its extension to other procedures in addition to registration and registration).

The process continues, according to the inquiry, so that once the appointment is activated, the citizen connects to the video session and a message is read out loud in which the authorization for the recording is collected of image (the content of the message and therefore the information provided to you for the collection of your consent is unknown).

Next, you show your DNI or relevant identity document, on both sides and once the identity has been verified by checking the data and the photograph shown, the procedure begins (it is not clear whether this process, which according to the DPD is that of "authentication", it is carried out using a facial recognition system that allows to verify that the photo of the document shown corresponds to the image of the person making the video call, as is done in the procedure defined by the Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of qualified electronic certificates, or if only makes a visual verification of the DNI or equivalent document, as would be done in a face-to-face process).

Regarding the documentation, it is indicated that it is provided "in an internal cloud and integrated into the videoconferencing platform, which connects to our cloud" and, as stated, "The public service managers are the who attend to the person and register the documentation they provide in the corresponding procedure, in the general register". It is not clear how the citizen provides the documents, if he does it later in a face-to-face procedure or does it by electronic means, and it is also not indicated what signature requirements are required for the documentation that is included in the file, if it is an electronic or handwritten signature.

The DPD asks "if this system can reliably guarantee the identity of the applicant, as it would be done in person or by means of a digital signature in the e-headquarters" and states that, "a priori it seems that there is sufficient legal guarantees, both for the verification system and for its storage in a secure environment, as indicated by the parameters of the National Security Scheme". And, likewise, that the system follows the example and requirements of Order ETD/465/2021, of May 6, which regulates remote identification methods by video for the issuance of electronic certificates qualified

The statement of reasons for the aforementioned order states: "(...) this Ministerial Order specifies the procedure to be followed for the remote video identification of an applicant, as well as the requirements and the minimum actions that lenders must take to detect attempts

of impersonation or the possible manipulation of the images or the data of the identity document.(...). Among other measures, it is required to verify the authenticity and validity of the identity document, as well as its correspondence with the applicant for the certificate. To do this, the remote video identification system used in the process must incorporate the necessary technical and organizational means to verify the authenticity, validity and integrity of the identification documents used, verify the correspondence of the holder of the document with the applicant performing the process, using technologies such as facial recognition, and verifying that this is a living person who is not being impersonated; all these requirements must be accredited, in the terms established by annex F11 of the ICT Security Guide CCN-STIC-140, of the National Cryptological Centre, through product certification. The reference to the Guide must always be understood to be made to the latest available version. It is also required that the staff in charge of verifying the applicant's identity verify the accuracy of the applicant's data, using the captures of the identity document used in the process, in addition to any other automatic means that can be implemented in remote video identification systems. To contribute to this end, it is planned to provide lenders with access to the intermediary platform of the Data Verification and Consultation Service, the body responsible for which is the Secretary of State for Digitization and Intel· Artificial intelligence, as a means of comparing the identity data of applicants with an authentic source, in line with the provisions of Commission Implementing Regulation (EU) 2015/1502, of September 8, 2015, on the setting of minimum technical specifications and procedures for the security levels of means of electronic identification in accordance with the provisions of article 8, section 3, of the aforementioned Regulation (EU) 910/2014."

At the outset, say that the purpose of the aforementioned order is identification for the issuance of qualified electronic certificates and that the requirements and guarantees established by the aforementioned order are suitable for this specific purpose. Any other procedure with a different purpose must be subject to the corresponding analysis that allows to determine, depending on the specific purpose that is to be achieved and the specific treatments that it involves, which requirements and guarantees are necessary.

Likewise, it must be clarified that it is not up to this Authority to define the means through which the identification of citizens is carried out by electronic means in the administrative process, since this corresponds to the public administrations, where appropriate, with the corresponding authorizations established by the regulations of administrative procedure. Also, it is not up to him to determine whether an identification system "can reliably guarantee the identity of the applicant". However, it is up to this Authority to ensure that these identification systems comply with the regulations for the protection of personal data and to determine the risks that their use may entail in the fundamental right to the protection of personal data.

III

From the point of view of the data protection regulations, the first question that needs to be analyzed regarding the data processing carried out by the system that is to be implemented consisting of the recording and conservation of citizens' images is its legality. And to do so, it is essential to determine whether it involves the processing of special categories of data.

In accordance with its articles 2 and 4.1, Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereinafter, RGPD) is applicable to any processing of personal data understood as 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". (Article 4.1 RGPD).

According to this definition, there is no doubt that the image and voice of a person, as well as the rest of the data contained in the DNI or equivalent document, are personal data.

The RGPD defines treatment as "any operation or set of operations carried out on personal data or sets of personal data, whether by automated procedures or not, such as collection, registration, organization, structuring, conservation , adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of enabling access, sharing or interconnection, limitation, deletion or destruction" (Article 4.2 RGPD) .

In short, the collection of this data from the people who undergo the identification process constitutes data processing that is subject to the principles and guarantees of the personal data protection regulations

Likewise, article 4.14) of the RGPD defines biometric data as "personal data obtained from a specific technical treatment, relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as facial images or fingerprint data".

It should be borne in mind that the RGPD includes biometric data in the category of data that must be subject to special protection when regulating the regime applicable to the treatment of this type of data.

Specifically, article 9.1 of the RGPD establishes that:

> **"1. The processing of personal data that reveal ethnic or racial origin, political opinions, religious or philosophical convictions, or trade union affiliation is prohibited, and the processing of genetic data, biometric data aimed at uniquely identifying a natural person, data relating to the health or data relating to the sexual life or sexual orientation of a natural person."**

Recital 51 of the RGPD specifies that "the treatment of photographs should not be systematically considered treatment of special categories of personal data, because they are only included in the definition of biometric data when the fact of being treated with specific technical means allows the identification or the univocal authentication of a natural person.)".

From the joint reading of these forecasts it is clear that the key element when considering the data relating to the physical, physiological or behavioral characteristics of a natural person

as biometric data is that these data are treated with specific technical means in order to uniquely identify or authenticate their identity. When this happens, we will be dealing with special categories of personal data.

On this matter, CNS Opinion 21/2020 which can be consulted on the Authority's website www.apdcat.cat analyzes when biometric data should be considered special categories of data.

In the case raised in the consultation, as already indicated, it is not clear whether specific technical means are used in order to uniquely identify or authenticate the identity of the citizen. However, it is indicated that the system follows the example and requirements of Order ETD/465/2021, of May 6, which regulates the methods of remote identification by video for the issuance of electronic certificates qualified

If the system implemented by the city council complies with the provisions of the aforementioned ministerial order, no doubt arises regarding the treatment of special categories of citizens' data, since facial recognition technology is being used for the purpose of uniquely authenticate your identity.

On the contrary, in a system in which the identity is authenticated by the public employee with the visual verification of the document shown, without the application of other technical measures that allow to uniquely authenticate their identity, it does not seem that can be considered a processing of biometric data and therefore special categories of data would not b

In short, depending on the technology applied to the system, personal identifying data of the interested parties or special categories of their data will be processed.

In both cases, the processing of personal data necessary for the implementation of the verification system, whether it deals with special categories of data or identification data of the citizen, must guarantee compliance with the principles provided for in article 5 of the RGPD.

IV

Article 5.1.a) of the RGPD establishes that the personal data collected must be treated lawfully, lawfully and transparently in relation to the interested party. In order for this treatment to be lawful, one of the conditions provided for in article 6.1 RGPD must be met, and in the case of special categories of data, the provisions of article 9 RGPD must also be taken into account.

Specifically, with regard to the treatments carried out by public administrations, paragraphs c) and e) of article 6.1 of the RGPD are particularly relevant, which respectively state that the treatment will be lawful if "it is necessary for the fulfillment of an obligation law applicable to the person responsible for the treatment", and "the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment".

As can be seen from article 6.3 of the RGPD and expressly included in article 8 Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), the processing of data it can only be considered based on the legal bases of article 6.1.c) i) of the RGPD when this is established by a rule with the rank of law.

Law 39/2015, of October 1, on the common administrative procedure of public administrations (hereafter LPAC), obliges public administrations to verify the identity of those interested in the administrative procedure by checking their first and last names or name or company name, as appropriate, that appear on the national identity document or equivalent identification document (article 9.1. LPAC).

Also, article 10.1 of the LPAC establishes:

> **"Generally, to carry out any action provided for in the administrative procedure, it will be sufficient for the interested parties to prove their identity beforehand through any of the means of identification provided for in this Law."**

For identification purposes, it is necessary to take into account what is established in article 1 of Royal Decree 1553/2005, of December 23, which regulates the issuance of the national identity document and its electronic signature certificates, which provides for:

> **"1. The National Identity Document is a personal and non-transferable document issued by the Ministry of the Interior that enjoys the protection that public and official documents are granted by law. Its owner will be obliged to keep and conserve it.**
>
> **2. Said document has sufficient value, on its own, to prove the identity and personal data of its holder that are recorded in it, as well as the Spanish nationality of the same. (...)**
>
> **4. Equally, the National Identity Document allows Spaniards who are of age and who enjoy full capacity to create the electronic identification of its holder, as well as to perform the electronic signature of documents, in the terms provided for in Law 59/2003 , of December 19, electronically signed.**
>
> **In the case of Spanish minors, or those who do not enjoy full capacity to work, the national identity document will only contain the utility of the electronic identification, issued with the respective certificate of authentication activated.**
>
> **5. The electronic signature made through the National Identity Document will have the same value with respect to the data entered in electronic form as the handwritten signature in relation to the data entered on paper. (...)"**

In the face-to-face procedure, the presentation of the DNI or equivalent identification document by the interested party to the public employee responsible for its processing constitutes sufficient guarantee for its identification.

Regarding identification by electronic means, the LPAC regulates the accepted systems. Thus the second, third and fourth sections of article 9 of LPAC establish:

"2. Those interested may identify themselves electronically to the Public Administrations through the following systems:

a) Systems based on qualified electronic certificates of electronic signature issued by providers included in the "Trusted list of providers of certification services".

b) Systems based on qualified electronic certificates of electronic seal issued by providers included in the "Trusted list of providers of certification services".

c) Concerted key systems and any other system, which the Administrations consider valid under the terms and conditions that are established, provided that they have a previous registration as a user that allows their identity to be guaranteed, prior authorization by the General Secretariat of Administration Digital from the Ministry of Territorial Policy and Public Function, which can only be denied for reasons of public security, prior to a binding report from the Secretary of State for Security of the Ministry of the Interior. The authorization must be issued within a maximum period of three months. Without prejudice to the obligation of the General Administration of the State to resolve in a timely manner, the lack of resolution of the request for authorization will be understood a

The Public Administrations must guarantee that the use of one of the systems provided for in letters a) and b) is possible for any procedure, even if some of those provided for in letter c) are admitted for that same procedure.

(...)
4. In any case, the acceptance of any of these systems by the General Administration of the State will serve to accredit against all Public Administrations, unless proven otherwise, the electronic identification of those interested in the administrative procedure"

For its part, Royal Decree 203/2021, of March 30, which approves the Regulation of action and operation of the public sector by electronic means, with regard to the identification and signature of citizens, establishes in its article 15 the following:

"(...)
3. Interested persons may use the following identification and signature systems in their electronic relations with Public Administrations:

a) According to the provisions of article 9.2 of Law 39/2015, of October 1, interested parties may identify themselves electronically to the Public Administrations through the systems described in letters a), b) and c) of said article In this last case the systems must be previously authorized by the General Secretariat of Digital Administration of the Ministry of Economic Affairs and Digital Transformation, which can only be denied for reasons of public security, after a binding report from the Secretariat of State of Security of the Ministry of interior

b) Likewise, the systems provided for in letters a), b) and c) of article 10.2 of Law 39/2015, of October 1, will be considered valid for the purposes of electronic signature before the Public Administrations.

c) In accordance with the provisions of article 10.4 of Law 39/2015, of October 1, when the applicable regulatory regulations expressly provide for it, Public Administrations may accept the identification systems provided for in said law as a signature system when they allow to accredit the authenticity of the expression of the will and consent of the interested parties. (...)

Any system of identification of those interested in the administrative procedure by electronic means that the public administrations wish to use and that is not based on qualified electronic certificates of electronic signature or electronic seal issued by providers included in the "Lista de confianza de prestadores de certification services", must be previously authorized by the General Secretariat of Digital Administration of the Ministry of Economic Affairs and Digital Transformation, notwithstanding that the acceptance of any of these systems by the AGE serves to accredit electronically to interested parties before all public administrations (article 9.4 LPAC)

On the other hand, it should be taken into account that in accordance with the provisions of the third paragraph of article 9 of LPAC:

"3. In relation to the identification systems provided for in letter c) of the previous section, it is established that the technical resources necessary for the collection, storage, treatment and management of said systems are located in the territory of the European Union, and in the case of special categories of data referred to in article 9 of Regulation (EU) 2016/679, of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons in the which respects the treatment of personal data and the free circulation of these data and therefore repeals Directive 95/46/CE, in Spanish territory. In any case, the data will be available for access by the competent judicial and administrative authorities.

The data referred to in the previous paragraph may not be transferred to a third country or international organization, with the exception of those that have been the subject of an adequacy decision by the European Commission or when the fulfillment of obligations so requires international assumed by the Kingdom of Spain."

In accordance with this regulation, the identification systems of the interested parties by electronic means referred to in letter c) of article 9.2 of the LPAC (Concerted key systems and any other system that the administrations consider valid and authorized by ministry) the technical resources necessary for the collection, storage, treatment and management of these systems are located in the territory of the European Union.

Likewise, it is necessary to take into account what is established in article 12 of the LPAC regarding assistance in the use of electronic media to those interested:

"1. The Public Administrations must guarantee that those interested can relate to the Administration through electronic means, for which they will make available the access channels that are necessary as well as the systems and applications that are determined in each case.

2. The Public Administrations will assist in the use of electronic means those interested not included in sections 2 and 3 of article 14 who so request, especially in relation to identification and electronic signature, submission of applications through the electronic register general and obtaining authentic copies.

Likewise, if any of these interested parties does not have the necessary electronic means, their identification or electronic signature in the administrative procedure can be validly carried out by a public official through the use of the electronic signature system provided for it. In this case, it will be necessary for the interested party who lacks the necessary electronic means to identify himself to the official and give his express consent for this action, which must be recorded for cases of discrepancy or litigation.

3. The General Administration of the State, the Autonomous Communities and the Local Entities will keep up to date a register, or another equivalent system, where the officials authorized for the identification or signature regulated in this article will be listed. These registers or systems must be fully interoperable and be interconnected with those of the remaining Public Administrations, in order to check the validity of the aforementioned qualifications.

In this register or equivalent system, at least, the officials who provide services in the registration assistance offices will be listed.

The processing of the personal data of those interested in the administrative procedure contained in the DNI or equivalent document, or in the electronic certificates accepted by the public administrations, necessary for their identification, both in person and electronically, will have as a legal basis the Article 6.1.e) of the RGPD in relation to Article 9 of the LPAC and Article 1 of Royal Decree 1553/2005, of December 23.

From the terms in which the query is formulated, it would be possible for the identification of the interested parties to be carried out in the system under analysis, through the presentation of their DNI or equivalent document to the official who is attending to them by video call and that, for the purposes of evidence, the video call is recorded and kept together with the rest of the documentation

In this case, given the obligation contained in the administrative procedure regulations to identify those interested in the administrative procedure, if the recording of the image and voice of the interested parties is carried out for the purpose of their identification, this treatment could also have as a legal basis the public interest provided for in article 6.1.e) of the RGPD in relation to article 9 of the

Likewise, if the purpose of the system is to assist interested parties who do not have electronic means, the legal basis would also be the public interest provided for in article 6.1. e) of the RGPD in relation to articles 9 and 12 of the LPAC

However, if the treatment involves the implementation of a facial recognition system that involves the treatment of biometric data of the interested parties, it must be taken into account that the RGPD prohibits in its article 9.1 the treatment of special categories of data, except if , in addition to a legal basis provided for in article 6.1, there are also some of the exceptions established in article 9.2 of the RGPD, including:

> **"(...)**
> **a) the interested party gives his explicit consent for the treatment of said personal data with one or more of the specified purposes, except when the Law of the Union or of the Member States establishes that the prohibition mentioned in the section 1 cannot be raised by the interested party; (...) g) the treatment is necessary for reasons of an essential public interest, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respecting the right to protection of data and establish appropriate and specific measures to protect the fundamental interests and rights of the interested party; (...)"**

It can be ruled out at the outset that the treatment of the biometric data of the interested parties for the purpose of identification in the administrative procedure can be based on the exception provided for in article 9.2.g) of the RGPD to the extent that it does not seem that, apart from the fact that this section requires the existence of a provision in the law of the European Union or in a rule with the rank of law, in this case the treatment can be based on the existence of a "public interest essential on the basis of the law of the Union or the Member States".

It is worth saying that the Constitutional Court has expressly ruled on article 9.2.g) of the RGPD in Judgment number 76/2019 of 22 May. In this judgment the court establishes criteria for what must be understood as essential public interest (by reference to STC 292/2000, in the sense that the restriction of the fundamental right to the protection of personal data cannot be justified , by itself, in the generic invocation of an undetermined "public interest"), of the requirements that must be met by the rule that regulates them in order to establish appropriate and specific measures to protect the fundamental interests and rights of the interested

Thus, the judgment analyzes these two requirements with regard to the exception provided for in article 9.2.g) in the following terms:

> **"The treatment of the special categories of personal data is one of the areas in which the General Data Protection Regulation has expressly recognized the Member States "room for maneuver" when "specifying their rules", as as it qualifies in recital 10. This margin of legislative configuration extends both to the determination of the enabling causes for the treatment of specially protected personal data - that is, to the identification of the purposes of essential public interest and the appreciation of proportionality of the treatment to the end pursued, essentially respecting the right to data protection - as well as the establishment of "adequate and specific measures to protect the fundamental interests and rights of the interested party" [art. 9.2 g) GDPR]. The Regulation contains, therefore, a specific obligation of the States**

members to establish such guarantees, in the case that enable them to treat specially protected personal data.

(...)

"The provision of adequate guarantees cannot be deferred to a time subsequent to the legal regulation of the processing of personal data in question. Adequate guarantees must be incorporated into the legal regulation of the treatment itself, either directly or by express and perfectly delimited referral to external sources that set the appropriate regulatory range. (...)"

In the absence of other exceptions to those provided for in article 9.2 of the RGPD, the processing of biometric data could be based on the consent of the interested parties when it meets the requirements established by the data protection regulations.

According to the RGPD, the consent of the interested party is: "any manifestation of free will, specific, informed and unequivocal by which the interested party accepts, (...), the treatment of personal data that concerns him; "(article 4.11 RGPD). In the case of special categories of data, moreover, consent must be explicit.

The RGPD outlines in recitals 32, 42 and 43 what are the requirements that consent must meet in order for it to be considered valid. Thus Recital 42 of the RGPD establishes that "For consent to be informed, the interested party must know at least the identity of the person responsible for the treatment and the purposes of the treatment for which the personal data is intended. Consent should not be considered freely given when the interested party does not enjoy true or free choice or cannot refuse or withdraw their consent without suffering any harm. Specifically, in the case of an imbalance between the interested party and the data controller, recital 43 states: "To guarantee that consent has been given freely, this should not constitute a valid legal basis for the treatment of personal data in a concrete case in which there is a clear imbalance between the interested party and the person responsible for the treatment, in particular when said person responsible is a public authority and it is therefore unlikely that consent has been given freely in all the circumstances of said particular situation. Consent is presumed not to have been freely given when it does not allow the separate authorization of the different personal data processing operations despite being adequate in the specific case, or when the fulfillment of a contract, including the provision of a service, is dependent of consent, even when this is not necessary for said compliance".

The European Council for Data Protection in Directives 5/2020 on consent in the sense of Regulation (EU) 2016/679, states with regard to consent in the treatments carried out by public administrations that:

"16. Recital 43 clearly indicates that it is not likely that public authorities can rely on consent to process data since when the person responsible for the treatment is a public authority, there is always a clear imbalance of power in the relationship between the person responsible for the treatment and the interested party. It is also clear in most cases that the interested party will not have realistic alternatives to accept the treatment (the treatment conditions) of said responsible. The ECPD

considers that there are other legal bases that are, in principle, more suitable for the treatment of data by public authorities.

17.Without prejudice to these general considerations, the use of consent as a legal basis for data processing by public authorities is not totally excluded under the legal framework of the RGPD. The following examples show that the use of consent may be appropriate in certain circumstances.

18. Example 2: A municipality is planning road maintenance works. Given that said works can disturb traffic for a long period of time, the municipality offers its citizens the opportunity to subscribe to an electronic mailing list in order to receive updated information on the progress of the works and on expected delays. The municipality makes it clear that there is no obligation to participate and asks for consent to use email addresses for this (only) purpose. Citizens who do not give their consent are not deprived of any basic service of the municipality or of the exercise of any right, therefore they have the capacity to freely give or deny consent to this use of the data. Information about the works will also be available on the municipality's website. (...)".

The consent of those interested in the administrative procedure cannot be understood as validly given in the context of the unequal relationship that occurs between the public administration and citizens if the refusal to give it entails some kind of adverse or discriminatory consequence.

Certainly, the impossibility of identifying oneself in front of the public administration for the completion of an administrative procedure that would lead to the refusal to give consent in the case at hand, would have adverse consequences for the citizen. However, if the citizen has other easily accessible channels enabled for this purpose (one of the electronic identification systems provided for in article 9.2.c) LPAC) and this system is voluntary for the interested party, no it seems that the free nature of consent can be questioned.

v

In addition to the principle of legality, any data processing must comply with the other principles established by the RGPD. Among these, the principles of purpose and minimization of data according to which personal data must be collected for specific, explicit and legitimate purposes (Article 5.1.b) RGPD) and must be appropriate, relevant and limited to that necessary in relation to the purposes for which they are treated (article 5.1.c))

In accordance with these principles, the controller, in this case the city council, must analyze what is the purpose of the processing of personal data and whether the data to be processed are adequate, relevant and not excessive in relation to that purpose.

As the TC has highlighted in repeated jurisprudence, by all Judgment 39/2016, of March 3, "the constitutionality of any restrictive measure of fundamental rights is determined by the strict observance of the principle of proportionality. For the purposes that matter here, it is enough to remember that to check if a measure restricts a right

fundamental exceeds the judgment of proportionality, it is necessary to ascertain whether it meets the following three requirements or conditions: if such a measure is likely to achieve the proposed objective (judgment of suitability); if, in addition, it is necessary, in the sense that there is no other more moderate measure for the achievement of such purpose with equal effectiveness (juicio de necesidad); and, finally, if it is weighted or balanced, more benefits or advantages can be derived from it for the general interest than damages on other goods or values in conflict (proportionality judgment in the strict sense) [SSTC 66/1995, of 8 May, FJ 5; 55/1996, of March 28, FFJJ 6, 7, 8 and 9; 207/1996, of December 16, FJ 4 e), and 37/1998, of February 17, FJ 8].” (FD.5)

The application of the principle of data minimization and the judgment of proportionality that it entails must take into consideration, in each case, the specific procedure in which the system is to be implen

It cannot be ruled out that for certain procedures the system may pass the judgment of proportionality. Thus, for example, as a system for identifying the interested parties provided for in article 9.2.c) of the LPA that has been authorized by the competent Ministry, or in the procedure for identifying and signing the documentation presented by the interested by a qualified official provided for in article 12.2 of the LPAC (whether this procedure is carried out in person at the municipal offices or remotely through a video call system).

Regarding this last procedure, the system would allow to record by electronic means the identity of the person who grants the express consent of the interested party provided for in article 12.2 of LPAC, so that the authorized official can sign electronically on his behalf using the electronic signature systems that the authorized official is equipped with (this consent should not be confused with consent under the terms of the data protection regulations).

Conversely, although there is not enough information available about the system referred to in the query, it does not seem that this can pass the judgment of proportionality in certain cases, such as for example for the electronic identification of an interested party who wants access the file in a face-to-face procedure (to leave an electronic record of your identification by the official), to the extent that in this case the direct verification of identity by the official would make it unnecessary to go to any other type of verification.

Thus, although the implementation of a facial recognition system could achieve the proposed purpose of unambiguously identifying the interested party in the administrative procedure and leaving evidence of this identification by electronic means (judgment of suitability), not it seems that it can overcome the judgment of necessity or the judgment of proportionality in the strict sense, to the extent that these measures involving the processing of special categories of citizens' data are not required for the identification of the interested party in the face-to-face procedure that it does not seem that more benefits can be derived for the citizen in the use of this system than the damage that would occur in their privacy due to the treatment of these special categorie

In any case, the determination of adequacy to the principle of data minimization and the overcoming of the proportionality judgment must be made in view of the specific procedure in which this identification system is intended to be applied.

It should be remembered that, depending on the risks that may be generated depending on the procedure in question, it may be necessary to carry out an impact assessment related to data protection (art. 35 RGPD) and, where appropriate, a prior consultation with the Authority (art. 36 GDPR).

VI

Finally, in the case that in the system referred to in the query, the identification of the interested parties is carried out without using means that involve the processing of special categories of data, the following considerations should be taken into account.

As explained, in this case the legal basis of the treatment could be found in article 6.1. e) of the RGPD in relation to article 9 of the LPAC, or in relation to article 12 of the LPAC (in the case of assistance to the interested party in the use of electronic media), provided that the system has been authorized by the competent Ministry.

It should be emphasized that the consent of the interested party referred to in article 12 of the LPAC when it regulates the assistance to the interested parties by electronic means should not be confused with the consent in terms of the protection regulations of data The purpose of the consent provided for in the aforementioned article 12 LPAC is to record the authorization granted by the interested party so that the authorized official can identify him and sign electronically using the electronic signature systems that the authorized official is equipped with .

Conclusions

It is not up to this Authority to define the means through which citizens are identified by electronic means in the administrative process, nor to determine whether an identification system can reliably guarantee the identity of the applicant.

A data subject identification system that collects together with the data of the DNI or identification document of the data subject his image and voice, may have as a legal basis the exercise of public powers conferred on the person in charge of the treatment in relation to the functions identification of those interested in the procedure provided for in the administrative procedure regulations.

If specific technical means are used that allow the unequivocal identification or authentication of a natural person, it will involve the processing of biometric data and therefore special categories of data. In order for this data processing to be lawful and appropriate to the data protection regulations, it must have the valid consent of the interested party and comply with the rest of the principles of the RGPD, among which the principle of minimization, so that given the specific circumstances of the procedure or procedures in which it is intended to be applied, it passes the judgment of proportionality.

Barcelona, January 24, 2022