PD 7/2018

**Report in relation to the Draft Decree establishing the electronic voting system in the processes of elections to bodies representing the administrative and technical staff at the service of the Administration of the Generalitat de Catalunya**

**The Draft Decree establishing the electronic voting system in the processes of elections to bodies representing the administrative and technical staff at the service of the Government of the Generalitat is presented to the Catalan Data Protection Authority Catalonia, so that the Authority issues its opinion on the matter.**

**The Draft Decree consists of a preamble, six articles and two additional provisions.**
**It is accompanied by the supporting report.**

**Having examined this Draft Decree and the documentation that accompanies it, and having seen the report of the Legal Counsel, the following is reported.**

**Background**

**Article 44 of the revised text of the Basic Statute of the public employee, approved through Royal Legislative Decree 5/2015, of October 30, provides that the procedure for the election of the Personnel Boards and for the election of the Staff Delegates will be determined by regulation, taking into account, among other general criteria, that the election must be made through personal, direct, free and secret suffrage that can be issued by mail or by other means telematic means (section 1.a)).**

**Currently, the electoral processes for representative bodies of personnel in the service of the Administration of the Generalitat of Catalonia are subject to regulation in Law 9/1987, of June 12, on representative bodies, determination of working conditions and participation of personnel in the service of public administrations and, additionally, the Royal Decree 1846/1994, of September 9, which approves the Regulations for elections to representative bodies of personnel in the service of the General Administration of the State.**

**Article 21 of Law 9/1987 provides that the corresponding public administration will facilitate the census of civil servants and the personal and material means for holding the elections.**

**The purpose of the Decree is exclusively to implement the electronic voting system in these electoral processes, with the purpose of encouraging participation and the exercise of the right to vote to voters, significantly eliminating costs in personal and material means, providing accessibility by avoiding travel, facilitate the exercise of the right for disabled people or people with reduced mobility, prevent errors in the voting process and ensure the speed and accuracy of the polls.**

**Legal foundations**

**I**

**(...)**

II

The purpose of the draft decree being examined is "the establishment of the electronic voting system for the elections to bodies representing the administrative and technical staff in the service of the Administration of the Generalitat de Catalunya" (article 1 ).

As this Authority has highlighted on previous occasions, from the perspective of the protection of personal data, in any electoral process that is held using electronic voting mechanisms, adequate management of the processed information becomes particularly important. In fact, it depends on this that the participation is real and effective. Only if the conditions under which the electoral process is carried out guarantee the correct identification of the people who participate, the confidentiality of their information - and, in particular, of their vote - and the security of all the information related to it, the freedom to participate and the reliability of the result are guaranteed.

In this sense, special mention should be made of the Opinion 3/2010 (available on the website http://apdcat.gencat.cat/), in which they are analysed, from the perspective of data protection, but also from a broader approach to information security, several issues related to the implementation of electronic voting systems that are of interest in relation to the Draft Decree being examined. Point out that everything that, in general, was highlighted in that opinion, remains valid, in particular, the sections relating to the risks of the different electronic voting systems.

Having said that, it is appropriate to assess in the present case the performance of the data protection impact assessment referred to in article 35 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 such data and which repeals Directive 95/46/CE (hereinafter, RGPD).

The RGPD requires an impact assessment on privacy "when it is likely that a type of treatment, in particular if it uses new technologies, by its nature, scope, context or purposes, entails a high risk for the rights and freedoms of physical persons"
(article 35.1).

In relation to this impact assessment, Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), lists, in its article 28.2, some cases in which 'understands likely the existence of a high risk for the rights and freedoms of people, such as "when the treatment could generate situations of discrimination, usurpación de identity or fraud, (...)" (letter a)), "when the processing could deprive those affected of their rights and freedoms or could prevent them from exercising control over their personal data" (letter b)), or "when the processing is not merely incidental or accessory to the special categories of data to the which refer to articles 9 and 10 of the Regulation (...)" (letter c)), among others.

It must be taken into consideration that, in the present case, the Project involves the processing of personal information which, although it would not strictly reveal the trade union affiliation of those affected, could lead to the revelation of their ideology. Therefore, it would involve the processing of data deserving of special protection (article 9.1 RGPD).

Considering the nature of the data processed, that its treatment may affect other rights such as the exercise of the right to vote, that losses of this information or inappropriate treatments of information linked to the electoral process could not only affect the result of the same but give rise to discriminatory or coercive situations for those affected, and that the

treatment could affect a wide number of people, this impact assessment should be carried out.

Article 35.10 of the RGPD establishes that if, in the procedure for approving the rule, the Project undergoes a privacy impact assessment, then it will not be necessary to carry out the assessment when the treatments are carried out n derivin

However, it should be noted that, in the present case, said impact assessment should include the assessment not only of the regulatory provisions on the electronic voting system established in the Project but especially the assessment of the specific technological solution chosen to carry out such voting. In other words, prior to the adoption of an electronic voting system, it would be necessary to carry out an assessment of the effect that said system may have on the privacy of the affected persons and an analysis of the different alternatives available to achieve the purpose pursued, so that one can opt for the one that offers more guarantees for people's rights.

Having said that, it should be noted that, in order to carry out a careful examination of the implications that, for the protection of the data of those affected, may arise from the implementation of an electronic voting system in the election process in what the Project mentions, it would have been convenient to have had said impact assessment at the time of issuing this report.

Finally, it should be noted that the Project mainly considers aspects and characteristics of existing electronic voting systems but does not properly describe the chosen technological option, so the examination will focus solely on these general aspects.

III

Having made these initial considerations, we now refer to the electronic voting procedure model that configures the Project.

According to article 2.2 of the Project, the electronic voting system consists of "the casting of the vote in electronic form remotely through a device connected to the Internet (...)". From what is inferred from article 6 of the Project, the voter can exercise the right to vote through an "Internet electronic voting platform".

From these forecasts and others contemplated in the explanatory memorandum that accompanies it (sections III to V), it seems clear that the voting procedure is configured as a remote electronic voting system, which the voter will be able to exercise through this "Platform", which you can access through the Internet, therefore, through your own devices (for example, a computer) and not through terminals facilitated and controlled by the corresponding authority in a given space.

However, the Project also contains several express references to the "digital ballot box" and the "electronic ballot box", which would be a specific element of face-to-face electronic voting systems.

Thus, article 2.2 of the Project provides that the vote "is stored in a cryptographically protected digital ballot box". Article 3.i) of the Project makes it clear that the voter, once the vote has been cast, can download a receipt from the system "that records the effective casting of the vote and its deposit in the electronic ballot box ( ...)". And article 5.1 of the Project, in relation to the functions attributed to the Coordinating Months, foresees that these supervise "the process of creating the digital ballot box" (letter a)), as well as being in charge of "the custody of the keys

cryptographic access to the digital ballot box that allow dissociated scrutiny of electronic votes" (letter b)).

As this Authority has agreed in Opinion 3/2010, previously mentioned, face-to-face systems and remote voting systems are two clearly differentiated models of electronic voting systems (FJ IV), which, from the perspective of the protection of data and the security model, may present particular risks in the various key phases of development of the voting procedure: identification and authentication phase; voting phase; information scrutiny and destruction phase; control or verification phase (FJ VI and VII).

For this reason, if, as it seems, the Project sets up an electronic voting procedure over the Internet as a remote voting system, it would be advisable to review the references made to the electronic or digital ballot box and replace them, if necessary, with those that correspond, for the purposes of clarifying the model configured by the Project.

IV

From the perspective of data protection, article 3 of the Project, which lists the guarantees of the electronic voting system, is particularly relevant.

These guarantees make express reference, among other issues, to the identification and authentication of the voter; to the secret nature of the vote and its integrity and uniqueness; the security of the electronic voting procedure; or the possibility of verifying its correct operation, as well as auditing it.

At the outset, these forecasts on which the Project is based must be positively assessed from the perspective of data protection and the security elements that must be taken into account in the design and implementation of the electronic voting procedure that is being examined, as required by the RGPD itself, which establishes data protection by design and by default (recital 78 and article 25).

Taking these guarantees as a starting point, given that the Project does not properly describe the electronic voting procedure, it is considered pertinent to point out:

- The importance of implementing sufficiently secure mechanisms and procedures when identifying people with the right to vote and providing them with the credential that should allow them to vote via the Internet, in order to avoid voting by people without right to do so, the impersonation of people who do have the right to do so, as well as the duplication of votes. In other words, to establish mechanisms that guarantee the correct identification and authentication of voters.

Regarding this, article 3 of the Project provides that the identification of the voter is guaranteed, on the one hand, "through the identification procedures of the corporate directory" (letter c)), and, on the other hand, his robust authentication, using “secure provisioning of corporate directory credentials” (letter g)).

In the explanatory memorandum that accompanies it, it is explained, in this regard, that "each registered voter has a certificate/access code to the application where the personalized selection of options and candidates is carried out" (section III) .

It seems clear from these forecasts that the system will only allow access to the voting platform to those people previously registered in the Generalitat's corporate directory, an aspect that must be positively assessed. However, with regard to the voter authentication process, it is not sufficiently clear whether this will be carried out through systems

based on electronic certificates or through mechanisms based on the attribution of a user and password.

In a case like the one examined, although the identification and authentication of the people with the right to participate in the electoral process would not pose major problems, from the point of view of data protection, if it were carried out through systems based on electronic certificates or electronic seals, given that these mechanisms offer sufficient guarantees, the use of mechanisms based on the attribution of a user and password cannot be ruled out either.

This type of mechanism is the most widespread method to prevent unauthorized access to systems or content within an information system. This is a measure established in international standards and certifications in the field of IT security (such as ISO/IEC 27001 on information security management) and also recognized by our legal system (for example, in Law 39/2015, of 1 October, on the common administrative procedure of public administrations (article 9)).

Point out that, in the event that this voter identification and authentication mechanism is chosen, care should be taken to establish a password management procedure that guarantees their confidentiality and integrity.

- The importance of adopting the appropriate measures to ensure that the vote cast by the person participating in the electoral process is unique, secret and anonymous.

Regarding this, article 3 of the Project expressly states that the system "does not allow establishing a link between the meaning of the vote and the person who cast it" (letter b)), it also guarantees that "the will expressed by the "voter is authentic, unequivocal and has not been altered either qualitatively or quantitatively" (letter d)) and that "the voter can cast a single vote and any possibility of duplicity or multiple votes by a same person" (letter e)).

It also provides that "the technical security of the information transmission and storage procedures is guaranteed, with measures that guarantee traceability and measures against additions, subtractions, manipulations, impersonations or misrepresentations of the voting procedure" (Article 3.f)).

And, at the same time, that "compliance with personal data protection regulations is guaranteed, applying high-level security measures in attention to the nature of the data" (Article 3.k)).

For its part, in the explanatory memorandum it is explained (section III), in this regard, that "the votes are encrypted in the voting devices and only the single electoral board can reconstruct the private key and decipher the votes. The process ensures that the correlation between the identity of the voters and the deciphered votes is broken (...). (...) the votes stored on the servers are cryptographically protected - encrypted and digitally signed - at all times, so no one can manipulate them, not even system administrators with privileged access - they do not have access to the private key-. (...) Free voting is also guaranteed - avoiding coercion or the sale of votes - with the vote receipt which is an alphanumeric code that does not reveal the voting option, that is to say, no voter can prove to third parties which is the meaning of your vote. (...)".

From the perspective of data protection, the prospect of implementing this set of security measures that would cover the different phases of the electronic voting process must be positively assessed.

Even so, it is necessary to warn, with regard specifically to the adoption of "measures that guarantee traceability" (article 3.f)), that these must only and exclusively allow to verify that

**a certain elector has exercised his right to vote by the electronic voting procedure. In other words, in no case should they allow establishing a link between the voter's identity and the meaning of his vote.**

**Although, it must be said, the Project foresees that the system does not allow such a link to be established (article 3.b)), the lack of concreteness on the scope of traceability in the present case makes it necessary to warn of this eventual risk for the secrecy of the vote and for other rights and interests of the affected person, such as the risk of being coerced based on the direction of their vote.**

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

**For this reason, it would be appropriate to modify the wording given in letter k) of article 3 of the Project, in which the application of "high-level security measures" is foreseen, in order to use a terminology adapted to the RGPD**

**In this regard, wording similar to the following is suggested:**

**"k) Compliance with the regulations on the protection of personal data, applying the technical and organizational measures that are necessary, taking into account the nature of the data and the severity and probability of the risks to the rights and freedoms of voters. "**

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

**In this regard, the aforementioned LOPDGDD provides that:**

> **"First additional provision. Security measures in the public sector.**
>
> **1. The National Security Scheme will include the measures that must be implemented in case of personal data processing, to avoid its loss, alteration or unauthorized access, adapting the criteria for determining the risk in the data processing to the established in article 32 of Regulation (EU) 2016/679.**
>
> **2. The responsible persons listed in article 77.1 of this organic law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of equivalent measures in the companies or foundations linked to them subject to private law.**
>
> **In cases where a third party provides a service under a concession, management assignment or contract, the security measures will correspond to those of the public administration of origin and will be adjusted to the National Security Scheme."**

**Point out that, among those responsible for the processing included in article 77.1 of the LOPDGDD, to which this DA1a expressly refers, we find the administrations of the autonomous communities, as well as their public bodies and public law entities, among others**

**Therefore, it must be borne in mind that, in the present case, in which the Project envisages the processing of data of administrative and technical staff at the service of the Administration of the Generalitat of Catalonia, the application of the established security measures in the National Security Scheme will be mandatory.**

**v**

**Still in relation to this article 3 of the Project, it should also be noted that this precept does not specify the conditions under which the personal data linked to the electronic voting procedure will be stored, beyond indicating the adoption of "technical" security measures ” in this respect (letter f)), which, according to the explanatory memorandum, consist of cryptographically protecting the servers. It is not known, however, whether these are own or third-party servers, as well as their location.**

**For this reason, the need to assess the existence of a possible treatment assignment (Article 4.8) RGPD), for example, in the case of contracting with a third party for the provision of hosting or information storage services related to the electronic voting procedure, including services that operate in the cloud. If this is the case, a processing contract should be formalized in the terms established in article 28.3 of the RGPD.**

**It would also be necessary to assess the existence of possible international transfers of data (hereinafter, TID), for example, in the event that the data is stored on servers located outside the territorial scope of application of the RGPD (Article 3) . If so, it should be taken into account that the TIDs would be subject to the regime provided for in articles 44 to 50 of the RGPD.**

**Point out, in this regard, that the RGPD provides that the EU Commission can decide that a third country, a territory or one or several specific sectors of a country, guarantees an adequate level of protection (article 45), whereby that there would be no inconvenience in being able to carry out the TID, as long as the other principles and obligations of the RGPD and the LOP**

**In the absence of this decision by the Commission, personal data could only be transmitted to a third country if adequate guarantees are offered and the interested parties have enforceable rights and effective legal actions (the RGPD establishes, in this regard, different mechanisms to consider that adequate guarantees are offered, such as binding corporate rules, standard clauses, certification mechanisms, etc. (article 46.2 RGPD)) or if any of the exceptions provided for in article 49 of the RGPD apply.**

**For more information on this specific issue, it may be of interest to consult the opinions CNS 5/2018 or CNS 6/2018, available on the Authority's website (http://apdcat.gencat.cat/).**

**VI**

**Article 5 of the Project establishes, in its section 1, the functions that, in relation to the electronic voting system, will correspond to the coordinating bodies, which include actions such as the supervision of the process of creating the digital ballot box (letter a )), the custody of the cryptographic keys to access the digital ballot box (letter b)) or the resolution of technological incidents (letter c)).**

**At the same time, it foresees that the coordinating meetings will have the support of a team of experts, in order to obtain the technical advice they require (section 2).**

**Without prejudice to valuing this forecast positively, it is necessary to bear in mind the need to guarantee that the personnel who make up the aforementioned coordinating bodies (Article 10 Royal Decree 1846/1994) will have sufficient technical knowledge to be able to correctly carry out the functions assigned to them. It should be remembered that a comprehensive security model, in which it is determined which security measures must be applied based on a risk analysis in the terms of the RGPD (recitals 83 and 84), also requires the adoption of organizational measures necessary and the implementation of training measures for the staff who must process personal data.**

**VII**

**Article 6 of the Project provides that "the Administration of the Generalitat de Catalunya, through the organs, bodies or entities that have been assigned the competences in matters of electronic administration, ICT and cyber security, provides advice and continuous support in these matters in order to guarantee the security and correct operation of the Internet electronic voting platform in all phases of the electronic voting procedure".**

**In this regard, make clear the need to define the conditions under which these third parties will participate in the electronic voting procedure and the consequences of this participation from the point of view of data protection.**

**Thus, it must be borne in mind that, to the extent that the provision of these advisory and support services involves the processing of personal data on behalf of the person responsible for the electoral process, a processing contract must be formalized in the terms established in article 28.3 of the RGPD.**

**VIII**

**Finally, positively evaluate the provision to inform the electors of the electronic voting system, the procedure for use and the applicable security measures through the official website of the electoral process (second additional provision).**

**Agree, in this regard, that this information must also include the set of aspects referred to in article 13 of the RGPD and that it must be provided in a concise, transparent, intelligible and easily accessible form , in clear and simple language (article 12 RGPD).**

**For all this the following are done,**

**Conclusions**

**Having examined the draft decree establishing the electronic voting system in the processes of elections to representative bodies of administrative and technical staff at the service of the Administration of the Generalitat of Catalonia, it is considered adequate to the forecasts established in the corresponding regulations on the protection of personal data, as long as the considerations made in this report are taken into account.**

**Barcelona, January 16, 2019**