PD 9/2019

Report on the Digital Administration Decree Project

Background

A letter from the Department of Digital Policies and Public Administration is being presented to the Catalan Data Protection Authority requesting that the Authority issue a report on the Digital Administration Decree Project.

Having analyzed the Project, and taking into account the current applicable regulations, and in accordance with the report of the Legal Counsel, I issue the following report.

Legal Foundations

I

(...)

II

The Project subject to report aims to regulate the organizational instruments, technological solutions, procedures and services involved in the operation of the digital services of the Administration of the Generalitat and other entities referred to in article 2 of the Project.

It should be noted at the outset that the operation of these services requires the processing of various information. Much of this information is not considered personal information, but it is undeniable that the operation of the digital administration will inevitably involve the processing of personal data. The considerations formulated in this report are directed exclusively to the treatment of this information.

The processing of information in the digital administration is based on the legal basis established in article 6.1.e) of Regulation (EU) 2016/679, general data protection (hereafter RGPD), according to which there is authorization for the treatment of personal data when "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 includes article 8 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereafter LOPDGDD), the data processing can only be considered based on the legal basis of article 6.1.e) of the RGPD when this is established by a rule with the rank of law.

Taking this into account, it is clear that the Decree under analysis does not constitute an instrument suitable for enabling the existence of new treatments, but it can specify the conditions under which treatments are carried out that are already provided for in rules with rank of law regulating the administrative procedure or other sectors of administrative activity. This would be the case, for example, of the provisions relating to interoperability, the right of citizens not to provide certain documents, the obligation to relate to the administration by electronic means or, in general, electronic processing of the administrative procedur

III

One of the aspects regulated in the project that has a direct impact on the right to the protection of personal data is what the project calls the "data governance model".

At the outset, and from a linguistic point of view, the appropriateness of the expression "data governance" can be questionable. This is not about analyzing or "governing" a single piece of data, but about establishing the governance of the data, which is multiple, not only in number but also in its diversity. For this reason, in line with the normative, jurisprudential and doctrinal texts on the matter, it would seem more appropriate to refer to "data governance".

On the other hand, it is surprising that article 4 of the project, when it lists the general principles of the Digital Administration, does not make any reference to the protection of personal data, considering that one of the purposes of the decree is to "establish the model of data gov Certainly perhaps a Decree is not the type of rule that should collect the applicable principles in a certain matter, and on the other hand, the applicability of the right to data protection, not only as a principle but as a true right, does not it depends on what is covered in this article. However, given the enumeration of principles that is made in this article, it seems that reference should also be made to the right to the protection of personal data and in particular to the principles of data protection in the design and data protection by default (art. 25 GDPR).

In the same vein, article 28.2 of the Project also does not refer to the protection of personal data as an element to be taken into account in the design of digital services.

Beyond this, article 10.1.a) of the Project provides that one of the criteria on which the data governance model is based is that "Data is a digital asset shared by the entire Administration of the Generalitat de Catalunya and its public sector, so its reuse must be maximized".

It must be taken into account that the processing of data by the Administration must respect, among others, the principle of purpose. (art. 5.1.b RGPD), according to which, personal data will be collected "for specific, explicit and legitimate purposes, and will not be subsequently processed in a manner incompatible with said purposes; in accordance with article 89, section 1, the further processing of personal data for archival purposes in the public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes ("limitation of the purpose") ;".

To this it should be added that article 6.4 of the RGPD allows data collected for a different purpose to be used for another purpose that is considered compatible in any of the cases provided for in the same section 4:

> **"4. When the treatment for a purpose other than that for which the personal data was collected is not based on the consent of the interested party or on the Law of the Union or of the Member States that constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives indicated in article 23, paragraph 1, the person responsible for the treatment, in order to determine whether the treatment with another purpose is compatible with the purpose for which the personal data were initially collected, will take into account, among other things:**
>
> **a) any relationship between the purposes for which the personal data have been collected and the purposes of the subsequent treatment provided; b) the context in which the personal data have been collected, in particular with regard to the relationship between the interested parties and the controller; c) the nature of personal data, in particular when special categories of personal data are treated, in accordance with article 9, or personal data relating to criminal convictions and infractions, in accordance with article 10; d) the possible consequences for the interested parties of the planned subsequent treatment; e) the existence of adequate guarantees, which may include encryption or pseudonymization."**

In other words, the data are collected for a specific purpose and, in principle, a provision that establishes that they are a digital asset shared by the entire Generalitat Administration and its public sector does not seem appropriate. The personal data are an asset of the persons who hold them (the affected persons) and the processing by the Administration of the Generalitat can only take place, by the competent body in each case, when one of the legal bases provided for in article 6 RGPD. This is without prejudice to its reuse when the personal data protection regulations allow it.

Although section 2 of article 10 expressly states that the data governance model is established in accordance with the principles and requirements provided for in the framework of the current data protection regulations, it would be advisable that the wording of article 10.1.a) reflects greater consistency with this regulation.

On the other hand, in letter f) it is also included as a criterion "Make the single data criterion effective through the collaboration between the different bodies and systems custodians of the same data and the unequivocal identification of the reliable source ."

Certainly, the principle of accuracy (art. 5.1.d) of the RGPD) requires that the information being processed is accurate and up-to-date. This must lead to the purification of that information that is not correct, either because it was initially no longer correct or because it has become out of date with the passage of time or due to the appearance of new circumstances.

However, together with this principle, the principle of purpose, to which we have already referred, must also be taken into account. That is to say, that the aforementioned project forecast will only be able to operate in areas in which the different data to be purged have been collected for the same purpose (art. 5.1.b) RGPD) or for a compatible purpose.

Likewise, it should be borne in mind that in some cases the single data criterion may not be valid. We think, for example, that regardless of whether the Administration may have a valid address for notification purposes (for example, the address where a certain natural person is registered), the administrative procedure regulations (art. 66.1.b) of Law 39/2015, of October 1 on common administrative procedure of public administrations (hereafter LPAC)) allows the physical place chosen for notification to be indicated by non-electronic means (when applicable). It is recognized as a right of the citizen, which would oblige to take into account several addresses for the purposes of notifications.
Also, for example, article 41.1 LPAC, allows the citizen to indicate an electronic device or an email address for sending notification notices in each procedure. Obviously this address can be a specific address for a certain procedure that does not match the one that can be used in other procedures. In these and other cases it does not seem that the single data criterion can be applied.

For this reason, it is proposed that a paragraph be added to article 10.1.f) to indicate that this mechanism can be applied "when appropriate".

Also in relation to the principle of purpose, it is also necessary to refer to article 12.1 of the project, according to which, "The data and documents of the people who have the subjects provided for in article 2 of this Decree, have to be used for the purpose of complying with the purposes, principles and actions provided for in this Decree...".

It should be noted that, from the point of view of the principle of purpose, the instruments, services and organizational and procedural provisions established in this decree do not constitute a purpose in themselves but are instruments at the service of another purpose (enforcing a right or obligation, offering a service, processing a procedure, etc.). For this reason, it would seem more appropriate to delete the words "purposes and principles" and refer only to the actions and instruments provided for in the Decree and the right of people not to provi

IV

Several forecasts of the Project allude to the regime of access to information. Thus, article 10.2 refers to the data governance model being established in accordance with the principle of "openness and public access to data" and article 19.1 refers to the "openness by default of all your data ".

Article 19 actually looks like it could refer to access to the data itself. If so, it would not make sense to regulate it within the section dedicated to interoperability, nor to use a concept such as "open data" to refer to a person's access to their own data

Although both article 10.2 and article 19.1 incorporate a reference to data protection regulations that should already lead to excluding personal information from access outside of the cases established by transparency legislation or sectoral legislation , the wording of these articles is contradictory and can generate some confusion. In terms of personal data, the "default" option can never be the opening of the data. And this not only because of the duty of confidentiality (art. 5.1.f) RGPD) but also because of the obligation to apply data protection by default (art. 25.2 RGPD). For this reason, it is recommended to review the wording of these two articles and other related ones, and replace it with a reference to which access to information must be carried out in accordance with the administrative procedure regulations and the which regulates transparency (including both active advertising and the right of access to information regulated in general or sectoral transpa

On the other hand, article 15 is headed "Access to open data" but then its content refers not only to open data but to data made available to other administrations. This can lead to confusion. On the other hand, it is not clear in the wording of this article the justification of the interconnection provided for between the data we have referred to and open data systems.

It should be noted in any case that Recital 31 of the RGPD expressly refers to some limitations regarding the interconnection of files of public authorities:

> **"(31) The public authorities to which personal data is communicated by virtue of a legal obligation for the exercise of their official mission, such as fiscal and customs authorities, financial investigation units, independent administrative authorities or supervisory bodies of the financial markets responsible for the regulation and supervision of the stock markets, should not be considered recipients of data if they receive personal data that is necessary to carry out a specific investigation of general interest, in accordance with the Law of the Union or the member states. Requests for communication from public authorities must always be submitted in writing, with reasons and on an occasional basis, and must not refer to the entirety of a file or lead to the interconnection of several files. The treatment of personal data by said public authorities must be in accordance with the data protection regulations that are applicable depending on the purpose of the treatment."**

v

Article 24 regulates the phases of archival management of data and digital assets. In letter c) the "Validity phase" is regulated, which starts from the end of the file and remains as long as the documents or data maintain the probative value of actions, rights and duties of the administration or citizens.".

Taking into account the uses provided for in this letter, it would be appropriate that with regard to personal data, a reference to the blocking duty provided for in article 32.2 of the LOPDGDD was incorporated.

Equally, and taking into account what is established in article 89 of the RGPD, it would also be convenient if letter d), relating to the historical phase, included some reference to the need to include blocking or some mechanism similar to blocking, as a guarantee for the adequate conservation of information that is maintained for archival purposes in the public i

As is known, Article 5.1.b) RGPD allows the processing and conservation of personal information for archival purposes in the public interest or for historical research purposes, so that it is not considered incompatible with the initial purpose for which was collected. However, Article 89 RGPD requires that appropriate safeguards be adopted. In the case at hand, an appropriate first guarantee should be the application of the minimization principle. In other words, keep only that part of the documentation or documentary series that is really justified for reasons of archiving in the public interest or historical research. But in addition, with respect to the information that must be kept, both to preserve its conservation in appropriate conditions and to guarantee that access occurs only by the people and the reasons that justify it, it could be of interest to foresee that a bloc

On the other hand, and also in relation to the preservation of documents, article 64.4 provides that "Citizen attention offices must eliminate, once they have been digitized, the paper documents that have been provided in these offices in accordance with the provisions of article 66 of this Decree.". Both documents that the person presenting the documents in person at the office wants to keep once they have been digitized should be excluded from this provision, as well as cases where original documentation is provided for the purposes of the administration making a copy authentic in the cases referred to in sections 4 and 5 of article 28 of the LPAC. This consideration would also be extended to article 66

VI

Article 33 of the Project regulates proactive and personalized services. It would be, as indicated in the same article, digital services whose purpose is to inform people, predictively and in advance, about the public services that can be accessed. The measure, which is based on the elaboration of profiles, constitutes an innovative use of technologies in public administration, to the point that in article 4.c) of the Project it is identified as one of the general principles of the 'Digital Administration. But given the breadth of information available to public administrations and the repercussions that an analysis of this type can have for people's privacy, it is necessary to take into account the requirements derived from data protection regulations, in particular, the principle of minimization, the principle of legality, the principle of purpose, and the conditions established for th Section 1 of article 33 includes a reference to the guarantee of the protection of personal data, but beyond that, the provisions of this article should be consistent with the provisions of this regulation.

It must be said that, precisely because it is a new service, the regulation contained in this article is not clear enough to be able to determine its scope and consequences, so in the analysis that n fa in this report will take into account the different interpretations or the different models to which, a priori, and without having an evaluation of

the impact on data protection, it seems that the current wording of the precept could result.

1) Principle of minimization

In accordance with the principle of minimization, only appropriate, relevant and limited data must be processed in relation to the purposes for which they are processed (art. 5.1.c).

It should be noted that in certain services, the possibility of offering information about other services or related procedures can be carried out without the need to create any type of profile. A first level of proactivity could already be achieved if the information offered, for example on the website of the administration in question, to people who present a certain type of request, without the need to make any kind of profile, information about other services or related procedures in which the people performing a certain procedure may be interested.

Thus, for example, the economic situation of the person who wants to undertake an economic activity would in principle be related to the start-up of the activity, but it would not seem justified that on the occasion of the application for the license of the activity and of the authorization to offer you personalized services, this could involve drawing up an economic profile obtained from the information that the administration has (taxes, penalties, deferral of taxes, information on social services, employment information, pensions, payroll if it was a public worker, etc.), to offer him the possibility of taking advantage of a certain line of subsidies or official credit. This information can be offered to the affected person without the need to prepare a previous financial profile.

It is also true that current technology allows that in other services, in which the relationship with the related information to be offered may not be so obvious, or in which the volume of information to be offered requires selecting it more carefully, it can be positive provide personalized inform But this does not mean that the possibility of offering these services should lead to admitting any type of profile.

For this reason, the article should not generally provide for the possibility of using profiling to offer this type of proactive services, but should provide that if the possibility of offering information does not require the profiling was not done. And in the case that it is justified to do them, they should be limited to the analysis of certain information that is predictable in relation to the service in question.

2) Principle of legality

As stated in section 3 of the same article, these services would be based on the creation of profiles based on the explicit consent of the persons affected or the existence of a rule with legal rank that has provided for it.

With regard to consent, if in general it is not necessary for the exercise of the public functions entrusted to the public administrations, it seems clear that, in the case at hand, the treatment that would be carried out to offer these services exceed the expectations that a citizen can have when he goes to the administration to carry out a certain procedure and can be highly intrusive in his life. These expectations

include the receipt of information related to the procedure carried out, but not related to other procedures in which the person may be interested based on a predictive analysis of the information he has provided to the Administration. For this reason, it may be legally appropriate to articulate these proactive services based on the consent of the affected persons. However, in accordance with article 4.1 RGPD this consent must be free, specific, informed and unequivocal. In addition, if the consent is used to create profiles (art. 22.2.c) RGPD) or to treat special categories of data (art. 9.2.a) RGPD), it must be explici

In order for the consent to be considered as free consent, the affected person must have a real ability to choose. In other words, that there are no negative consequences in your relationship with the administration for not having given your consent. This implies that in a case like the one proposed in this article, the citizen should be able to choose to receive the information in a non-personalized, easy and accessible way.

But in addition, the consent must be specific. In other words, the citizen must know with a sufficient level of concreteness what he is consenting to, so that he can foresee the consequences of consent. In the regulation, it is not sufficiently clear neither the origin of the information that will be used to prepare the profiles, nor what aspects will be analyzed in the profiles.

According to section 6 of the article, the information from which the profile would be drawn up would be collected in forms. It would seem, according to this first interpretation, that the information from which the profile would be drawn up would be the information included in these forms associated with specific procedures and that would be used to offer information on related services. If so, this would facilitate control by the citizen of the information that will be taken into account when making the profile and would also contribute to having control over the type of profile that can be drawn up.

However, the forecasts contained in sections 2 and 4 of article 33 of the Project seem to indicate the opposite. At the outset, article 33.4 regulates a digital register or equivalent system that collects the data relating to consents and that guarantees consultation by all the bodies referred to in article 2 of the project. This suggests that the citizen's consent would not refer only to other services related to the service referred to in the form in which he consented, but to any other information in the possession of the administration, whether it be the collection on the occasion of the procedure in question, whether c

For its part, section 2 of article 33 of the project provides that proactive services can be based on personal information obtained for the same purposes or for different purposes. And not only for the administration or agency itself, but, as it seems to follow from the provision of article 33.4 of the project, other subjects can also use that authorization to offer their own services.

It should be borne in mind that the Administration has a lot of information on all aspects of our lives (residence, family relationships, economic, professional, employment information, training, infringements and sanctions, crimes and misdemeanors, etc.) which usually also includes special categories of data (health, social services, certain aspects of sex life or sexual orientation, biometric data, etc.). It does not appear that consent, even

could be a suitable legal basis to allow the elaboration of profiles with all this magnitude, since it is very difficult for the citizen to be able to foresee the scope of his consent, especially if techniques are used in the elaboration of these profiles of artificial intelligence.

On the other hand, in a case like the one we are dealing with, the specific character of the consent must also be predicated with respect to the aspects that are intended to be evaluated in the profile, so that the citizen can know which aspects of his life will be evaluated .

Although the possibility that when submitting a certain request or carrying out a certain procedure consent can be requested to offer proactive services linked to the procedure carried out by the affected administration, and based on the information linked to this procedure, could be admissible to the extent that the citizen would know the information that will be analyzed to create the profile, as well as the specific purpose of creating the profile, it would not be so if it is intended to use this qualification to collect any other type of information about this person that is in the possession of the administration or those included in arti

The data protection regulations allow consent for different matters to be collected in the same declaration using what is called granular consent, so that the consent regarding each of these matters is clearly differentiated and not conditioned by the remainder However, in an environment like the one analyzed here, where it is very difficult for the citizen, and even for the administration itself, to anticipate what the scope and consequences of an evaluation of multiple aspects of people's lives, it does not seem that a priori it can be justified, even if there is granular consent, a service that offers the possibility of enabling the administration to evaluate and draw up profiles that include all aspects of life of the people about whom the administration has information.

With regard to the possibility that it is a law that provides for a proactive service in a certain area, this is a possibility that could be protected in the legal basis provided for in article 6.1.e) RGPD. However, it must be borne in mind that this rule, apart from determining the purpose pursued (which must be sufficiently specific and which could not cover the processing of any information available to the administration) must fulfill a public interest and must of being proportionate to the purpose pursued (art. 6.3 RGPD). Apart from this, article 6.3 RGPD also foresees that this rule may contain other provisions such as the general conditions that govern the legality, the types of data subject to treatment, the interested parties affected, the entities to which the data and the purpose of the communication, the limitation of the purpose as well as, among others, the measures to guarantee lawf

Accordingly, any law that creates a certain proactive service will have to take these forecasts into account. And it could hardly be concluded that a law providing for the preparation of profiles for this purpose would be provided without specifying where the information would be obtained to make the profile and what aspects are evaluated.

It would be even more problematic if this type of service were to be applied to profiles that involve the processing of special categories of data (art. 9 RGPD). In this case it must be taken into account that according to articles 22.4 and 9.1.g) RGPD it is necessary not only that a law provides for it, but that it must obey reasons of essential public interest and must

foresee appropriate and specific measures to protect the fundamental interests and rights of those interested, as recalled by the recent Constitutional Court Judgment 76/2019 of May 22 in relation to article 58 bis of Organic Law 5/1985, of 19 of June, of the general electoral regime, incorporated by the LOPDGDD.

3) Purpose principle

In accordance with the purpose principle, the data are collected for specific, explicit and legitimate purposes and must not be subsequently processed in a manner incompatible with these purposes (art. 5.1.b) RGP

The data available to the administration have been collected for a specific purpose. It cannot be ruled out that these data are then used for other compatible purposes, as recognized by Articles 5.1.b) and 6.4 GDPR. However, wording such as that incorporated in article 33 of the Project does not seem compatible with this principle, according to which the data held by the administration (and we have already referred to the breadth and diversity of the information that the administration may have on people) may end up being used to create profiles of all citizens who relate to the administration for various and unspecified purposes. It would therefore be necessary to take into account, case by case, the criteria established in article 6.4 RGPD to determine compatibility.

It should be specified that the purposes for which the information will be used are related to that purpose for which the information subject to evaluation was collected and that, in addition, they will be compatible with the purpose for which was collected.

4) Elaboration of profiles

Data protection regulations recognize the right of individuals not to be the subject of an automated decision, including the creation of profiles that produce legal effects on the affected person or that significantly affect them (art. 22 RGPD). The creation of profiles is only allowed, with a certain exceptional character, in the three cases provided for in article 22 and with the requirements and guarantees contained therein.

Bearing in mind that in the case at hand the purpose of profiling is only to offer personalized information, that is to say, to inform the affected people about the public services that may affect them in a more predictable way, it would not seem that in principle the creation of profiles should entail legal effects on the people affected. However, it cannot be ruled out that depending on the information processed, the type of service to which it refers, and the rest of the concurrent circumstances, a treatment of this type may have significant effects on the people affected (for example the information received may condition the exercise of your rights), in which case the provisions of article 22 RGPD should be taken into account.

Article 22 RGPD allows the creation of profiles whether they are based on the explicit consent of the persons affected or if it is provided for by a rule with the rank of law.

Regarding consent, we have already referred above to what requirements consent should meet in order to be an adequate consent for the purposes of articles 6 and 9 RGPD, and these same requirements must apply in order to consider it a suitable consent

for the purposes of article 22 RGPD. In addition, however, it should be borne in mind that Article 22.3 RGPD requires that the citizen has the right to obtain human intervention, to express his point of view, to contest the decision and obliges the person in charge to adopt the appropriate measures to safeguard the rights, freedoms and legitimate interests of the interested par

Regarding the possibility that it is a law that provides for a proactive service in a certain area, this is a possibility foreseen in article 22.2.b) of the RGPD. However, the same section 2.b) also provides that the legal norm must provide for adequate measures to safeguard the rights, freedoms and legitimate interests of the interested party.

Aside from the possibility of revoking consent at any time in cases where it is based on consent (33.4.2 of the project), which in reality would not be an additional guarantee but a legal requirement (art. 7.3 RGPD), for with regard to guarantees, paragraph 6 of the same article 33 foresees two types of guarantees:

a) On the one hand, it provides that the data collection forms or systems must include informative clauses that explain in a clear and accessible way the use of the data, as well as the other mandatory information in accordance with the data protection regulations (this would include not only the provisions of article 13 and where applicable 14 of the RGPD, but also what is provided for in article 22.3 RGPD when it is based on consent). Therefore, it would not be an additional measure but it would be about complying with an obligation that already follows from the RGPD.

b) On the other hand, it is foreseen that the data collection forms or systems must also include the possibility of objecting (it would be good to clarify that the possibility of objecting would apply to cases in which the proactive service based on a profile has been provided for in a standard with the rank of law). Taking into account what is established in article 22.2.b) RGPD it would be good to foresee not only the possibility of exercising the right of opposition, which is actually already provided for in article 21.1 RGPD, but to establish a system of opt out, so that the citizen could decide directly, without the need for any other justification, to stay out of th

In conclusion, the wording of this article should be revised in order to collect that the offer of proactive services will only be based on the creation of profiles when there are circumstances that justify it. And when it is admissible, the regulation should be clearer and more detailed. Both in the cases in which the offer of proactive services is based on consent, and when it is based on a law, it should be foreseen that only information related to the procedure in which it will be used for the elaboration of the profile consent has been given and that the aspects to be evaluated and the information to be offered proactively must always refer to services or procedures related to the procedure or service from which the information has been collected and that are compatible with the purpose for which the data was collected. This, in addition to excluding certain categories of data such as special categories of data, relating to infractions and administrative sanctions or the commission of crimes or misdemeanors, etc. or to provide adequate guarantees based on the type of information analyzed and the existing risks, such as for example the provision of an opt-out system, for cases in which the personalized service has been established in a standard with a range of law, in addition to offering sufficient and understandable information about the scope and consequences that can be derive

In any case, considering that this type of service involves obtaining profiles through automated systems, which involves an innovative use of technology in the field of public administration, which may have an impact on the exercise of people's rights, that it cannot be excluded that this involves large-scale treatment (depending on the number of services and the people who are ultimately affected by them) and that, in addition, the wording of the Decree does not foresee the exclusion of the categories of specially protected data, before launching each of these services (and before approving the corresponding law in the case of proactive services provided for in the laws) it would be necessary to carry out a assessment related to the impact on data protection (AIPD) in accordance with the provisions of arti

For these purposes, it is recommended to consult the Guide on impact assessment related to data protection in the RGPD (2.0) available on the Authority's website.

VII

Article 53 of the project regulates the mass presentation (more than ten) of requests or writings on the same matter.

The article regulates both the presentation forms and the entry entry in the register, but does not regulate the notification of the resolution or resolutions that may be issued by the Administration.

In this regard, it should be borne in mind that article 40.5 of the LPAC states that "Administrations may adopt the measures they consider necessary for the protection of personal data contained in administrative resolutions and acts, cuando estos tengan por destinatarios a más from an interested party."

In accordance with this, it should be foreseen that, regardless of whether the submission of applications was simultaneous, the personal information that may be contained in the resolution, may only affect some of the interested persons, with which what should be foreseen are the appropriate mechanisms to guarantee that the rest of the people who participate in the mass presentation do not have access to information that does not affect them, unless all the people interested consent to the communication to the rest.

VIII

In chapter 4, dedicated to identification and electronic signature, article 56.3 refers to when for reasons of "legal security" it is necessary to use a signature system that "anonymizes" the identity of the public employee , other electronic signature systems must be determined.

At the outset, the reference to "legal security" seems wrong, given that it should only refer to "security".

On the other hand, and from the point of view of data protection regulations, the use of the term "anonymity" does not seem appropriate, given that although in this case the person signing would not be identifiable by third parties, he would it would be at least by the entity that manages the alternative electronic signature system and by the administration to which the public employee belongs. For this reason, it is recommended to use the expression "preserve identity".

Apart from these issues, it could be good to introduce in this article an express reference to the possibility of using a pseudonym in these cases.

On this issue, it should be borne in mind that Law 59/2003, of December 19, on electronic signatures (hereafter, LSE) establishes that recognized digital certificates must include, among other information, "the identification of the signatory, in the case of natural 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 legal persons, by its name or company name and its tax identification code" (article 11.2.e)).

In view of this precept, the identification of the signatory in the configuration of the certificate recognized by the certification service provider in these cases could be carried out by means of a pseudonym, which could consist of an identification number (for example, the TIP number for members of the Mossos d'Esquadra Corps) that cannot be associated with a specific person by third parties.

Still related to the electronic signature, in article 57.2 an issue is regulated that in reality would not be related to the signature (as the article seems to announce) but to the requirements for the implementation of an automated administrative action . Among the requirements that must be established in the resolution of the competent body, a reference to the requirements derived from Article 22 RGPD for automated decisions involving the processing of personal data is missing.

On the other hand, it is recommended to revise the wording of article 60, since the expression "The record in the processing of data of the Electronic Headquarters..." is difficult to understand.

IX

Article 69 establishes that the transmission of the administrative file to the interested persons is the making available to the Electronic Headquarters or personalized space of the Headquarters.

It should be borne in mind that article 82 of the LPAC establishes that in the process of hearing the interested persons, the limitations provided for in Law 19/2013, of December 9, will be taken into account. Accordingly, a provision should be incorporated in this project article to accommodate the possibility that access to the file may be partial. For these purposes, a provision similar to the following could be included: "The system for sending the administrative file to the interested persons is the making available of the file or the appropriate part of it, to the Electronic Headquarters or personalized space...".

X

Article 79 of the project refers to the Contact Database. At the outset, it is necessary to make a linguistic observation, given that the expression "... the Generalitat has a corporate data processing...", does not seem to be adequate. Data processing (art. 4.2 GDPR) is carried out, or is intended to be carried out, but is not available. For this reason, it would be more appropriate to refer to "... the Generalitat must have a corporate database...". Similar considerations can be made regarding the seventeenth additional provision of the Project.

Aside from this linguistic issue, the second section of article 79 contains a description of the data that will be included in this database for the purposes of sending notices of making notifications available, to identify through the system of agreed key to send communications in the administrative procedure and to manage other notices. This database seems to be related to the provision of article 13.3 of Law 29/2010, of August 3, on the use of electronic media in the public sector of Catalonia, although neither the purposes nor the types of data included fully match. It would therefore be necessary to adapt this article to the provisions of Law 29/210.

On the other hand, the considerations that have already been formulated in Legal Basis III of this report regarding article 10.1.f) of the Project are reproduced here, especially taking into account that the seventeenth additional provision provides, in addition , the interconnection with other contact databases that have the bodies established in article 2.1 of the Pr

Also in relation to this issue, the eighteenth additional provision provides that within one year from the entry into force of the decree, citizens obliged to communicate electronically with public administrations must communicate the contact details to be incorporated into this database. According to what has been set out in Legal Basis II of this report, it seems that the rule that should provide for this data communication obligation should be a rule with the status of law.

Conclusions

Having examined the Digital Administration Decree Project, it would not be contrary to the provisions established in the personal data protection regulations if the considerations made in this report are taken into account, in particular those contained in the legal basis VI.

Barcelona, July 29, 2019