

Report in relation to the Draft order approving the application of the Public Procurement Services Platform and the integrated electronic bidding tools, the Digital Envelope and the Electronic Tender

Background

It is presented to the Catalan Data Protection Authority the Draft order approving the application of the Public Procurement Services Platform and the integrated electronic bidding tools, the Digital Envelope and the Electronic Tender, in order for the Authority to issue its opinion.

The Draft Order consists of an explanatory part, ten articles, an additional provision, a repealing provision and a final provision.

Having analyzed the Project and the file that accompanies it, in view of the current applicable regulations, and in accordance with the report of the Legal Counsel, the following is reported.

Legal Foundations

I

(...)

II

The Draft Order being examined aims to approve a new version of the Public Procurement Services Platform (PSCP) application, which constitutes "*the single and complete point of reference for the dissemination of information of the activity related to public procurement and the contractor profiles of all the contracting bodies of Catalonia*" (article 1.1).

It also aims to approve the new application of the electronic tendering tools that the PSCP has integrated, of Digital Envelope and Telematic Offer, which constitute "*electronic mechanisms for sending and keeping proposals in public procurement procedures securely until that the opening conditions are given that allow access to its content, with the aim of providing Catalonia's contracting bodies and companies with tools to carry out the tendering process by electronic means with legal and technical guarantees*" (article 1.1).

The first version of the PSCP application had been approved by Order ECF/313/2008, of June 23, with the purpose of "*constitute the tool of information and provision of services*

related to public procurement in Catalonia, as well as being the central point of information on aspects related to tenders, awards and others related to public procurement" and, subsequently, new functions have been gradually incorporated, such as through Order VEH/172/2017, of July 25, with respect to which it is foreseen to be expressly repealed, once the present draft order (derogatory provision).

From the point of view of data protection regulations, the use of the PSCP and the services that are integrated into it involves the processing of certain personal data, understood as "all 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) of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereinafter, RGPD)).

To point out that the data relating to legal entities are excluded from this scope of protection, as specified by the RGPD itself by establishing that "the protection granted by the present Regulation must be applied to natural persons, regardless of their nationality or location of residence, in relation to the processing of your personal data. This Regulation does not regulate the processing of personal data relating to legal entities and in particular to companies established as legal entities, including the number and form of the legal entity and its contact data" (recital 14), but not the data of natural persons who provide services in a legal entity and data relating to individual entrepreneurs and liberal professions.

Therefore, its treatment, as well as that of the data of public workers and holders of contracting bodies carried out through the aforementioned applications, must comply with the provisions of the RGPD and of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD).

In this sense, the explicit reference made to the data protection regulations in articles 5 and 9 of the Project should be positively assessed, without failing to highlight the importance of taking data protection into account from the design and by default in the implementation of these types of applications, as provided in article 25 of the RGPD.

Having said that, it should be noted that this report is issued exclusively with regard to the assessment of the impact that the Draft Order may have from the point of view of the protection of personal data, for which reason it is mentioned below exclusively of those aspects of the Project that are considered relevant in view of the provisions of the data protection regulations.

III

Article 2 of the Draft Order provides the following:

"2.1 All contracting bodies in Catalonia publish their contractor profiles through the PSCP.

2.2 The corporate electronic bidding tools integrated into the PSCP are available to all contracting bodies in Catalonia that have their contractor profiles registered there .”

In accordance with this provision, the different contracting bodies in Catalonia must use the PSCP for the publication of their contractor profile and, therefore, for the dissemination of that information related to their contractual activity. Also, through the PSCP, they have the bidding tools that are integrated into it for the electronic processing of the corresponding procurement files.

Remember that, despite the obligation to use the PSCP, each of the contracting bodies remains responsible for the processing (Article 4.7) RGPD) of the personal information they have in the exercise of their functions in the field of public procurement, as well as also of that information included in his profile as a contractor resident in the PSCP and that he must disseminate in compliance with the advertising obligations established both in the public sector contract regulations and in the transparency legislation.

With regard to the body responsible for the PSCP, it will act as data controller with respect to the data properly associated with the operation of the PSCP and the services provided through it.

And, in the event that the technological solutions to be able to provide these services come from third parties, these could have the status of data processors (Article 4.8) RGPD) if their action involves having to process personal information on behalf of the body responsible for the PSCP.

Responsible for the treatment is understood as *"the natural or legal person, public authority, Service or other organism that, alone or together with others, determines the purposes and means of the treatment"* (article 4.7 RGPD).

The person in charge of the treatment is understood as *"the natural or legal person, public authority, service or other organism that processes personal data on behalf of the person responsible for the treatment"* (article 4.8 RGPD).

From the point of view of data protection, the definition of what is the role of the different actors involved in the processing of personal data always becomes an essential element to determine the obligations and responsibilities that may correspond to each of them (for example, when complying with the duty of information or attending to the rights to informative self-determination, etc.).

Bearing this in mind, point out that it would be possible for the same order to clarify these issues by establishing the responsibilities of the various agents involved. This, without prejudice to having to formalize, if applicable, the corresponding data controller contract under the terms of article 28.3 of the RGPD.

The Draft Order describes in detail the functionalities offered by the PSCP (article 3.3 and 3.4) and also the functionalities of the electronic tender service (article 7.3).

The main function of the PSCP is to facilitate the dissemination (and, therefore, consultation) of information on the activity relating to public procurement and the contractor profiles of all the procurement bodies in Catalonia, which will also cover the dissemination of certain personal data (article 4.1) RGPD), basically identifying data of both bidders and the successful tenderer, natural persons, as well as the public workers involved by reason of their position or duties.

The PSCP will also allow, among other services, *"the generation of a file with the data of active publications so that it can be consulted from the Open Data Portal"* (article 3.5).

Given this, it is not superfluous at this point to refer to the recommendations made by this Authority in opinions CNS 57/2016 (prior to the validity of the RGPD), CNS 58/2018 and CNS 1/2019, which complement each other with the opinion CNS 12/2020, regarding the application of the principle of data minimization (Article 5.1.c) RGPD) in the publication of this type of information for the purpose of fulfilling the obligations of active advertising that imposes public sector contract regulations, as well as transparency regulations. The aforementioned opinions are available at the following link on the [Authority's website](#).

With respect to those functions described which result in the possible collection of personal information (subscription services for notices, use of web forms for tender registration, etc.), remember the importance of respecting the principles of transparency (articles 5.1.a) RGPD) and data minimization (article 5.1.c) RGPD).

Thus, it must be taken into consideration that, in application of the principle of transparency, it will be necessary to provide the affected persons with information on the conditions and circumstances relating to the processing of their data, in a concise, transparent, intelligible and easily accessible manner (article 12 GDPR). Specifically, it will be necessary to provide the information referred to in article 13 of the RGPD, which could be delivered by layers or levels, under the terms of article 11 of the LOPDGDD.

With respect to the principle of data minimization (Article 5.1.c) RGPD), it must be borne in mind that the personal data collected from the means enabled by the PSCP must be adequate, relevant and limited to what is necessary to achieve the until they justify their treatment in each case.

V

Articles 4 and 8 of the Draft Order regulate the integration of the PSCP and the electronic bidding tools, respectively, with certain corporate applications of the Generalitat de Catalunya and the AOC Consortium.

Section 1 of article 4 foresees the possibility that the PSCP, apart from being integrated with the applications related to it, can be integrated *"with other applications or systems"*.

The RGPD defines data processing 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, diffusion or any other form of enabling access, comparison or **interconnection**, limitation, suppression or destruction" (article 4.2)).*

It is therefore appropriate to remember that the integration of the PSCP with other information systems that involve a flow of information containing personal data must be carried out respecting the principles established in the RGPD, in particular the principles of legality (article 5.1.a)), data minimization (article 5.1.c)) and limitation of purpose (article 5.1.b)).

VI

The Draft Order provides that access to the part of the PSCP application that allows the publication of information, as well as to the own space of the bidding companies, and also access to the bidding tools electronics that are integrated into the PSCP requires the prior authentication of the users.

Specifically, article 3.2 provides the following:

"3.2 The authentication of all users who access the part of the application for use by the Administration (Publication Manager) is carried out through the Identity Manager and access control to corporate resources of the Generalitat (GICAR) or through the identity management tool of the extranet of the Catalan administrations (EACAT), which is managed by the Consorci Administració Oberta de Catalunya (Consorci AOC). Information publishing functions require access with a qualified or recognized public worker digital certificate, validated by the AOC Consortium. The public part of the PSCP is not subject to access control, except for the space owned by the bidding companies. Access to registration and specific management from this space requires authentication through the VALid service of the AOC Consortium."

And article 7 provides the following:

"7.1 The corporate electronic bidding tools are accessible to users of the contracting bodies through the PSCP's electronic address. The authentication is carried out, in the same terms established in article 3 of this Order (...). The corporate e-bidding tools are accessible to the bidding companies from the specific electronic address of the virtual bidding space in PSCP of each file in which they have been established as tools for the submission of bids on Digital envelope or the online offer. (...)."

These forecasts are positively valued, given that, from the point of view of data protection, it is necessary, among other actions in the field of security, to adopt appropriate mechanisms that allow the correct identification and authentication of users of the PSCP and of the services that are integrated, for the purposes of guaranteeing, as required by the RGPD, that no unauthorized treatments will occur (Article 5.1.f)).

Remember, with respect to the different user profiles of the PCSP that may be established with different functions and responsibilities, that the system must incorporate the necessary mechanisms to guarantee that the access of these users will only take place with respect to that information that is necessary for the development of the functions attributed to them, in compliance with the principle of data minimization (article 5.1.c) RGPD).

Apart from the establishment of identification and authentication mechanisms, the draft order incorporates throughout its articulation and especially in articles 5 and 9 specific forecasts on the adoption of security measures appropriate to the risks detected (article 32 RGPD), for the purposes of guaranteeing the integrity and confidentiality of information (Article 5.1.f) RGPD) in the implementation of the PSCP and electronic bidding tools, particularly with regard to online communications with users and also with other information systems with which the PSCP is integrated, which should be evaluated positively.

These measures include, among others, the use of electronic headquarters certificates, digitally secured application device (CDA) certificates, secure communication protocols that include the encryption of exchanged data, secure repositories, establishment of incident records and traceability of the different actions carried out by users, the use of antiviruses, the establishment of physical security policies and measures, as well as the use of an availability probe that allow alerting of possible service drops.

It is also planned to carry out compliance audits and follow up on the associated action plans to resolve the non-compliances that are identified.

In addition to all this, the Draft Order expressly provides that both the PSCP and the electronic bidding tools *"are subject to compliance with the National Security Scheme (ENS) and the personal data protection regulations and guarantee of digital rights"* (articles 5.4 and 9.5, respectively).

Certainly, the application of the security measures established in the ENS in this case is mandatory by application of the first additional provision of the LOPDGDD, which provides the following:

*"1. The National Security Scheme will include the measures that must be implemented in the 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 what is established in the 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 the security measures to be implemented in a case like the one under consideration should also include the proper training of the staff who must process the personal data in question.

conclusion

examined the Draft order approving the application of the Public Procurement Services Platform and the integrated electronic bidding tools, the Digital Envelope and the Telematic Offer, is considered adequate to the provisions established in the regulations on protection of personal data.

Barcelona, February 8, 2023

Machine translation