CNS 31/2018

Opinion in relation to a consultation of a local administration body on the external contracting of Data Protection Delegate services

A letter from (...) is presented to the Catalan Data Protection Authority in which it considers whether it is possible to proceed with the external contracting of the services of a Data Protection Delegate and, if so, what guarantees must be adopted in this regard .

Having analyzed the request and the documentation that accompanies it, and having seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

As stated in the consultation letter, Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereafter, RGPD) will be fully applicable next May 25, so it is necessary to adapt to the forecasts of this new regulation.

One of the novelties that the RGPD incorporates in the area of personal data protection is the figure of the Data Protection Delegate (hereinafter, DPD).

Article 37 of the RGPD regulates its designation, in the following terms:

"1. The person in charge and the person in charge of the treatment will appoint a data protection delegate provided that: a) the treatment is carried out by a public authority or body, except the courts that act in the exercise of their judicial function; b) the main activities of the person in charge or the person in charge consist of processing operations that, due to their nature, scope and/or purposes, require regular and systematic observation of interested parties on a large scale, or) the main activities of the person in charge or the person in charge encargado consist of the large-scale processing of special categories of personal data in accordance with article 9 and of data relating to convictions and criminal offenses referred to in article 10.

2. A business group may appoint a single data protection officer as long as he is easily accessible from each establishment.
3. When the person responsible for the treatment is a public authority or body, a single data protection officer may be appointed for several of these authorities or bodies, taking into account their organizational structure and size.

4. In cases other than those contemplated in section 1, the person in charge or the person in charge of the treatment or the associations and other organizations that represent categories of persons in charge or persons in charge may appoint a data protection delegate or must appoint him if so required by the Law of the Union or of the Member States. The Data Protection Officer will be able to act on behalf of these associations and other organizations that represent those responsible or in charge.
5. The data protection officer will be appointed based on his professional qualifications and, in particular, his specialized knowledge of law and

practice in the field of data protection and its capacity to perform the functions indicated in article 39.

6. **The data protection delegate may form part of the staff of the person in charge or of the person in charge of the treatment or perform their functions within the framework of a service contract.**

7. The person responsible or the person in charge of the treatment will publish the contact details of the data protection officer and will communicate them to the control authority."

For its part, article 38 of the RGPD specifies the position of the DPD in the organizational structure of the person in charge and of the person in charge of the treatment, in the following terms:

"1. The person in charge and the person in charge of the treatment will guarantee that the data protection delegate participates adequately and in a timely manner in all issues related to the protection of personal data.
2. The person in charge and the person in charge of the treatment will support the data protection delegate in the performance of the functions mentioned in article 39, facilitating the necessary resources for the performance of said functions and access to personal data and treatment operations , and for the maintenance of their specialized knowledge.

3. The person in charge and the person in charge of the treatment will guarantee that the data protection delegate does not receive any instructions regarding the performance of said functions. The person in charge or the person in charge will not be dismissed or sanctioned for performing their functions. The data protection officer will report directly to the highest hierarchical level of the person in charge.
4. Interested parties may contact the data protection officer for all questions related to the processing of their personal data and the exercise of their rights under this Regulation.

5. The data protection officer will be obliged to maintain secrecy or confidentiality in the performance of his duties, in accordance with the Law of the Union or of the Member States.

6. The data protection officer may perform other functions and tasks.
The person responsible or in charge of the treatment will guarantee that said functions and tasks do not give rise to a conflict of interest."

Finally, article 39 of the RGPD determines the specific functions of the DPD, establishing that:

"1. The data protection delegate will have at least the following functions: a) inform and advise the person in charge or the person in charge of the treatment and the employees who deal with the treatment of the obligations incumbent upon them by virtue of this Regulation and other protection provisions data from the Union or member states; b) supervise compliance with the provisions of this Regulation, other data protection provisions of the Union or Member States and the policies of the person in charge or of the person responsible for the treatment in the area of personal data protection, including the assignment of responsibilities, the awareness and training of the personnel who participate in the treatment operations, and the corresponding audits; c) offer the advice requested about the impact assessment related to data protection and supervise its application in accordance with article 35; d) cooperate with the control authority; e) act as the point of contact of the control authority for issues related to the treatment, including the prior consultation referred to in article 36, and make inquiries, as the case may be, on any other matter.

2. The data protection officer will perform his duties by paying due attention to the risks associated with processing operations, taking into account the nature, scope, context and purposes of the processing."

It follows from this legal regulation, for the purposes of interest in the present case, that:

a) All public administrations and their linked or dependent public bodies, which act as responsible or in charge of the processing of personal data, must mandatorily appoint a DPD (article 37.1.a) RGPD).

This designation should occur before May 25, the date on which the RGPD will be fully applicable (Article 99.2 RGPD).

b) It is possible to designate a single DPD for several of these administrations and public bodies. It will depend on their organizational structure and size (article 37.3 RGPD).

However, it cannot be ruled out that, in complex administrative structures, it is more appropriate to have several DPDs.

c) The DPD can be a public administration worker (internal DPD) or the services offered by a professional or an organization/company outside the public administration organization (external DPD) can be contracted (article 37.6 RGPD).

Therefore, the DPD can be a natural person or a legal person.

d) The DPD can perform its functions full-time or part-time (article 38.6 RGPD).

In public administrations, departments or large public bodies in which there is a single DPD, this can perform the functions full-time and can count, if necessary, with the support of a work team or a unit specifically dedicated to the Data Protection.

In public administrations, departments or public bodies of medium or small size, this DPD will probably carry out his functions by combining them with others (part-time DPD).

In the specific area of local administrations, it is possible that the dimensions and resources of these organizations make it unfeasible to have a DPD integrated into the staff (internal DPD), either full-time or part-time. Therefore, it might be common to have an external DPD.

It is also possible in these cases to appoint the same DPD to share between different authorities or public bodies (Article 37.3 RGPD).

e) It must be guaranteed that the DPD acts, at all times, with independence (article 38.3 RGPD), so it is necessary to avoid any possible conflict of interest in the exercise of DPD functions (article 38.6 RGPD).

The conflict of interest may arise in those cases in which a part-time internal DPD is chosen. Given that the DPD acts as an internal adviser and supervisor of GDPR compliance, as well as serving as a point of contact and interlocutor between the organization, data protection authorities and interested parties (Articles 38.4 and 39.1 RGPD), it seems clear that it cannot at the same time perform other incompatible functions, in the sense that it involves participating in decision-making about the existence of data treatments or about the way in which these data must be treated.

As highlighted by WG29 (Guidance Document on DPDs, 13 December 2016, revised 5 April 2017 (WP243, rev.1)), managerial or command jobs but also other lower positions in the organizational structure

that intervene, directly or indirectly, in the processing of personal data, even positions of legal representation, are areas in which conflicts of interest can potentially or objectively arise. Therefore, it should be avoided to accumulate these tasks with those of the DPD (for example, if secretaries, auditors or treasurers are designated as DPD or the person in charge of ICT or information security, a conflict of interest).

However, it cannot be ruled out that a conflict of interest may arise if an external DPO is appointed. In this sense, WG29 points out, in said document, that, in the case of outsourcing the provision of the service to a company or team of professionals, it is essential that each of the people in this organization who exercise the functions of DPD fulfill all the requirements referred to in articles 37 to 39 of the RGPD. In particular, it emphasizes that none of these people have a conflict of interest and, in order to avoid this, it proposes as good practice that tasks within the DPD team are clearly assigned and appoint a single person as contact and person in charge of each client (in this case, of each administration, department or public body).

It should be borne in mind that, in this case of outsourcing the service, the conflict of interests could also arise, even, with the own company or organization when it already provides the person in charge with other services in the field of data protection that involve the making of decisions on the way in which the data must be treated (for example, having a consultancy or a professional office specialized in the provision of services aimed at complying with the legislation on the protection of personal data , such as conducting audits, among others).

f) It is necessary to publish the contact details of the DPD and communicate them to the control authority (article 37.7 GDPR).

Given the special "triangular" position of the DPD, which, as has been said, acts as an interlocutor between the interested parties, the public administration (responsible or in charge) and the control authority, it is necessary to provide information that allow you to easily and directly contact them.

IV

In view of these considerations, it is clear that local public administrations must appoint a DPD (article 37.1 RGPD), as well as that there are no drawbacks for, for this purpose, proceeding with the contracting of the services provided by a third party, be it a natural or legal person (article 37.6 RGPD).

However, it must be borne in mind that, in these cases (external DPD), it is equally necessary to accredit the professional competences of the DPD referred to in article 37.5 of the RGPD (legal knowledge in the field of data protection and also in of technology applied to data processing), to which it would be necessary to add knowledge of administrative order and procedure.

It is also necessary to guarantee that a conflict of interest will not be incurred (article 38.6 RGPD) and this whether the services provided by a professional are contracted or the services provided by an organization/ company outside the organizational structure of the Public administration. If you opt for the latter option, it would be necessary, for this purpose, to individualize the provision of services in a worker of the company or of the team of professionals who is singled out as DPD of the Administration (which, as s 'has seen, it could be assisted by other professionals from this company or team).

Also, given that the DPD, in the exercise of their functions, must be able to access the data being processed (Article 38.2 RGPD), a processing order should be formalized between the Administration and the contracted third party (the professional or the organization/company), in the terms

established in article 28.3 of the RGPD, so that the DPD can access the personal information for which the Administration is responsible, necessary for the performance of its functions.

The mentioned article 28.3 of the RGPD provides that:

"3. The processing by the controller will be governed by a contract or other legal act in accordance with the Law of the Union or the Member States, which binds the controller with respect to the controller and establishes the object, duration, nature and purpose of the processing, the type of personal data and categories of interested parties, and the obligations and rights of the person in charge. Said contract or legal act will stipulate, in particular, that the controller: a) will treat personal data solely following the documented instructions of the controller, including with respect to transfers of personal data to a third country or an international organization, unless it is obliged to it by virtue of the Law of the Union or of the Member States that applies to the person in charge; in such a case, the manager will inform the person in charge of that legal requirement prior to the treatment, unless such Law prohibits it for important reasons of public interest; b) will guarantee that the persons authorized to treat personal data have committed to respect confidentiality or are subject to a confidentiality obligation of a statutory nature; c) will take all the necessary measures in accordance with article 32; d) will respect the conditions indicated in sections 2 and 4 to resort to another treatment manager; e) will assist the person in charge, taking into account the nature of the treatment, through appropriate technical and organizational measures, whenever possible, so that he can comply with his obligation to respond to requests aimed at the exercise of the rights of the interested parties established in chapter III; f) will help the manager to ensure compliance with the obligations established in articles 32 to 36, taking into account the nature of the treatment and the information available to the manager; g) at the choice of the person responsible, will delete or return all personal data once the provision of the treatment services is finished, and will delete the existing copies unless the conservation of personal data is required under Union Law or member states; h) will make available to the person in charge all the information necessary to demonstrate compliance with the obligations established in this article, as well as to allow and contribute to the performance of audits, including inspections, by the person in charge or another auditor authorized by said responsible

4.5.2016 L 119/49 Diario Oficial de la Unión Europea ES In
relation to what is provided in letter h) of the first paragraph, the manager will immediately inform the person in charge if, in his opinion, an instruction infringes this Regulation or other provisions in data protection matter of the Union or of the Member States."

In relation to the subscription of this processing assignment, it may be of interest to consult the Guide on the controller in the RGPD prepared by the data protection authorities to assist controllers and processors in adapting to the requirements of the RGPD, available on the Authority's website http://apdcat.gencat.cat/ca/inici/.

On the other hand, the designation of the DPD as well as their contact details should be made public on the Administration's website (article 37.7 RGPD).

This data should also be recorded in the informative clauses (articles 13.1.b) and 14.1.b) RGPD) that are provided to the affected persons, as well as in the Register of processing activities that must be drawn up by the 'Administration (Article 30.1.a) RGPD).

Regarding the information to be provided, it should be noted that, as pointed out by GT29 (Guidelines document on DPDs, already cited), it is not required that the contact details of the DPD subject to dissemination include their first and last names. In view of the functions carried out by the DPD (article 39 RGPD), it is necessary to provide information that allows the interested parties to contact them easily and directly, a purpose which it is understood could be achieved by publishing a telephone number, a postal address (optionally, a post office box could be added) and, if available, a specific email address (this could also consist of a URL that allows access to an application or an electronic form to contact them). This, without prejudice to the fact that the dissemination of the name and surnames may also be enabled, if deemed appropriate.

All this also without prejudice to the DPD's obligation to identify themselves to the people they attend to in the exercise of their functions if they so request, in accordance with article 53.1.b) of Law 39/2015 , of October 1, of the common administrative procedure of public administrations.

On the other hand, despite not being required, in view of the functions attributed to the DPD, it would be advisable to communicate their identity and contact details to the employees of the Administration (for example, through their Intranet).

Finally, it would also be necessary to notify this Authority of the designation of the DPD through the corresponding form, available at the Authority's electronic headquarters https://seu.apd.cat/ (article 37.7 RGPD)

In this form, the identification data of the person who will act as DPD can be entered, in which case it is necessary to inform them in advance of the communication of their data to the Authority.

Point out that it will also be necessary to notify the Authority of any modification that affects this designation, such as a change in the contact details of the DPD or the termination of the contract for the provision of services, through the corresponding form (also available at the electronic headquarters of the Authority).

In accordance with the considerations made so far in relation to the query raised, the following are made,

Conclusions

The person in charge of the treatment can contract the DPD services offered by a professional or an organization or company outside their organizational structure (article 37.6 RGPD), as long as the professional skills referred to in the RGPD are proven and the no concurrence of any conflict of interest (Article 38.6 RGPD).

The designation of this external DPD also requires the formalization of a processing commission contract, in the terms established in article 28.3 of the RGPD, so that it can access the personal information for which the Administration is responsible, necessary for to the development of their functions.

Once the DPD has been designated, their contact details must be published in such a way that interested persons can contact them easily and directly (article 37.7 RGPD), as well as communicate this designation to this Authority.

Barcelona, May 28, 2018