CNS 31/2020

Opinion in relation to the query made by a city council on the return and destruction of personal data once the provision of a municipal service has ended

A letter from a city council is presented to the Catalan Data Protection Authority in which it is requested that the Authority issue an opinion on the return and destruction of personal data linked to the provision, under the concession modality, of the early childhood education service at the municipal kindergarten, once the provision of this service has been completed.

Specifically, it proposes:

a) How to list and request the return and destruction of data to the person in charge of the treatment, and what supporting documents must be presented by the person in charge of the treatment of data for the return and destruction of all documents, physical and electronic supports that has generated during the provision of the service.

b) Which document and how must the person in charge prove that the copies he keeps while responsibilities can be derived from the assignment of the provision are properly blocked.

The consultation is accompanied by the contractual clauses which enable the aforementioned public service concessionaire entity, in charge of the treatment, to treat on behalf of the city council, responsible for the treatment, the personal data necessary for its provision.

Having analyzed the request, and seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

The City Council states in its consultation that, on March 13, 2015, it signed an administrative management contract with a foundation to provide, under the concession modality, the service of the first cycle of early childhood education in the home of municipal children, for 3 school years with the possibility of 2 extensions until the 2019-2020 academic year.

Also that, following the approval of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), on October 17, 2019, the City Council and the entity concessionaire of the aforementioned public service signed new contractual clauses, which authorizes the entity, in charge of the treatment, to treat on behalf of the City Council, responsible for the treatment, the personal data necessary for the provision of the service.

The fifth transitional provision of the LOPDGDD states that:

"The contracts of treatment manager signed prior to May 25, 2018 under the provisions of article 12 of Organic Law 15/1999, of 13

of December, of Protection of Personal Data will remain in force until the expiry date indicated therein and, in the event of an indefinite agreement, until May 25, 2022.

During these periods, any of the parties may require the other to modify the contract so that it complies with the provisions of Article 28 of Regulation (EU) 2016/679 and Chapter II of Title V of this law organic."

Given that the assignment contract formalized between the City Council and the foundation has been adapted to respect the provisions of Article 28 of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27 2016, General Data Protection Regulation (RGPD), as well as the LOPDGDD, it should be borne in mind that this will be the applicable regime.

III

As can be seen from article 28.3 of the RGPD, the regulation of the relationship between the person in charge and the person in charge of the treatment must be established through a contract or a similar legal act that binds them .

This contract or legal act must specify the object, duration, nature and purpose of the treatment, the type of personal data and the categories of interested parties, as well as the obligations and rights of the person in charge. It must also stipulate that the person in charge:

"a) will treat personal data solely following the documented instructions of the person in charge, including with respect to the transfer of personal data to a third country or an international organization, unless it is obliged to do so 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

In relation to what is provided in letter h) of the first paragraph, the manager will immediately inform the manager if, in his opinion, an instruction violates this

Regulation or other provisions on data protection of the Union or the Member States."

In accordance with this precept of the RGPD, when a person in charge decides to establish a treatment order, as would have taken place in the present case, one of the issues that must be determined in the contract is the destination of the data at the end of the order in question (article 28.3.g) RGPD).

On this issue, article 33 of the LOPDGDD establishes that:

"3. The person in charge of the treatment will determine whether, when the provision of the services of the person in charge ends, the personal data must be destroyed, returned to the person in charge or delivered, as the case may be, to a new person in charge.
The data will not be destroyed when there is a legal provision that requires its conservation, in which case they must be returned to the person responsible, who will guarantee their conservation as long as this obligation persists."

That is to say, when a person in charge makes an order for the treatment, it must be foreseen in the corresponding contract if, once the provision of the service has been completed, the person in charge must proceed with the deletion or return of the personal data and any existing copy, either to the controller or to another agent designated by the controller.

However, the data will not be destroyed when there is a legal provision that requires its conservation, in which case the data will have to be returned to the person responsible, who must guarantee its conservation as long as this obligation persists.

Point out, at this point, that the processing agreement or contract must clearly establish which of the possible options the person in charge has chosen as the destination of the data, as well as the form and term in which must fulfill

IV

Having examined, in the terms set out above, the contract for the processing formalized between the City Council and the public service concessionaire, it should be noted that the clause relating to the destination of the data once the provision of the service has been completed provides for both the return of the data to the person in charge as well as its destruction by the person in charge:

"j) Destination of the data:

Return the personal data and, where appropriate, the media containing them, once the service has been completed, to the person in charge of the treatment.

The return must involve the destruction of the copies and the total erasure of the existing data on the computer equipment used by the person in charge.

However, the person in charge may keep a copy, with the data properly blocked, as long as responsibilities can be derived from the performance of the service.

Destroy the data, once the service has been completed. Once destroyed, the person in charge must certify the destruction in writing and must deliver the certificate to the data controller.

However, the person in charge may keep a copy, with the data properly blocked, as long as responsibilities can be derived from the performance of the service.

Both forecasts, which are contradictory, can generate certain doubts about what is the specific action that in this case the person in charge must carry out with said data once the provision of the awarded service has been completed. In other words, it is not clear whether the person in charge should return the data to the City or proceed with its destruction.

Despite this, in accordance with the applicable regulations, it can be said that, in the present case, by virtue of the principle of continuity of public services, it may be necessary to return the data linked to the provision of the service to the City Council, responsible for treatment.

As we have seen, the destruction of the data is not relevant when there is a legal provision that requires its conservation (article 33.3 LOPDGDD, second paragraph).

According to the information available (clause two of the contract), the data linked to the provision of the first cycle of early childhood education services in the municipal kindergarten refer in this case to the students of the center and their parents or legal guardians

These are identifying data (name, address, photograph, ID), personal characteristics data (date and place of birth, nationality, sex), economic and financial data (bank data) and special categories of data (health data and data relating to needs special education). In other words, data that usually make up the records of the students, in this case, of the municipal center.

At this point, reference must be made to the provisions of Law 10/2001, of July 13, on files and documents.

This Law extends its scope of application to "all the documents of public ownership in Catalonia, the private documents that make up or can make up the Catalan documentary heritage, the archives located in the territorial area of Catalonia and the administrative bodies that give them support" (article 3).

In accordance with article 6.1 of Law 10/2001, those produced or received in the exercise of their duties, among others, are public documents (in the terms of article 2.a)) the private concessionaire institutions of public services, in what refers to these concessions (letter g).

According to article 9 of Law 10/2001, "once the active and semi-active phases are concluded, the evaluation regulations must be applied to all public documents, on the basis of which the conservation, for reasons of cultural, informative or legal value, or elimination. No public document can be removed if the regulations and procedure established by regulation are not followed."

In any case, it is up to the person in charge of the treatment, the City Council, to determine what information needs to be kept and therefore the information that the person in charge of the treatment must deliver to the City Council to guarantee the continuity of the service.

With regard to the personal records of students in municipal kindergartens, as seems to be the case at hand, it will be necessary to take into account, in this sense, what is established in the document evaluation table 708, approved by the Order CLT/152/2014, of April 30 (DOGC 6627). This TAD establishes, in relation to said information, the retention period of one year from the end of the file, at which point its total destruction must proceed.

If, therefore, there is a legal obligation to preserve this type of information, in this case what would correspond, according to the aforementioned regulatory provisions, is for the person in charge to return the data and, where appropriate, the media in which they are contained in the 'City Council once the provisi

first cycle service for children in the municipal kindergarten. It would be up to the City Council to guarantee its conservation during the aforementioned period.

v

With regard to the way of articulating the return of the data to the City Council, an issue to which the consultation refers, it must be said that the data protection regulations do not establish any specific provision in this regard.

It is therefore up to the person in charge to determine in the commission contract the form and the period in which the person in charge must comply with this provision.

It is recommended that, before the formal act of receipt or compliance with the fulfillment of the object of the contract, the obligation to return the personal data linked to the provision of the service in question is communicated to the person in charge of the treatment, in attention to what is established in the corresponding treatment contract and in accordance with the applicable regulations, to which reference has been made.

It would also be good to indicate to the person in charge of the processing that said return must cover both the data that the City Council initially communicated to him and those that he was able to prepare from this data or those that he subsequently collected on behalf of the City Council. That is to say, all that personal information that may be contained in the personal files of the students of the municipal kindergartens or linked to the operation of the service.

Remember, at this point, that the return or return of the data must be carried out by adopting the appropriate measures to guarantee adequate security, particularly for the purposes of avoiding, during its transfer or transfer to the City Council , unauthorized or illegal access, as well as its loss, destruction or accidental damage (article 5.1.f) RGPD).

Security measures that should in any case meet the criteria established in the National Security Scheme (ENS), approved by Royal Decree 3/2010, of January 8.

This is clear from the first additional provision of the LOPDGDD:

> **"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."**

For the purposes of certifying the return of said information, the signature by the person in charge of 'a document in which he declares or records the delivery of all the personal information he has as a result of the provision of the service on behalf of the City Council, as well as that the copies have been destroyed and the erasure

total of the existing data on their computer equipment. This, without prejudice to what is set out below.

VI

It should be noted that the public service concessionary entity, in charge of the treatment, can keep a copy of the data linked to the provision of this service, duly blocked, in order to attend to possible responsibilities arising from the treatment, while these responsibilities have not prescribed

This is clear from article 33.4 of the LOPDGDD:

> **"4. The person in charge of the treatment will be able to keep, duly blocked, the data as long as responsibilities could arise from their relationship with the person in charge of the treatment."**

According to article 32.2 of the LOPDGDD, the blocking consists of "the identification and reservation of the same, adopting technical and organizational measures, to prevent their treatment, including their visualization, except for making the data available to the judges and courts, the Fiscal Ministry or the competent Public Administrations, in particular the data protection authorities, for the requirement of possible responsibilities derived from the treatment and only for the prescription period of the same."

Section 4 of this article 32 of the LOPDGDD specifies that "when for the fulfillment of this obligation, the configuration of the information system does not allow blocking or an adaptation is required that involves a disproportionate effort, a copy will be made security of the information in such a way that there is digital evidence, or of another nature, that allows to prove the authenticity of the same, the date of the blocking and the non-manipulation of the data during the same."

Once blocked, the data may not be processed for any purpose, except for making the data available to judges and courts, the Public Prosecutor's Office or the competent public administrations, in particular the data protection authorities, for the requirement of possible responsibilities derived from the treatment (article 32.3 LOPDGDD).

Upon completion of the data blocking period, which may vary depending on the information processed and the responsibilities that may be generated for the person in charge of the treatment, the data must be effectively deleted (article 32.2 LOPDGDD).

With regard to the way in which the person in charge must prove that he keeps the data properly blocked, a matter expressly referred to in the query, it must be said that the data protection regulations do not establish any provision in this regard, only that the person in charge of the treatment must offer sufficient guarantees in terms of specialized knowledge, reliability and resources, with a view to the application of technical and organizational measures that meet the requirements of the RGPD, including the security of the treatment (considering 81 RGPD) and that, to demonstrate this, adherence to codes of conduct (Article 40 RGPD) or possession of a data protection certificate (Article 42 RGPD) serve as evidence mechanisms (Article 28.5 RGPD) .

In any case, the documentation that the person in charge has generated to implement the security measures established in the commission contract, intended to fulfill the obligations of data protection legislation (as would be the case of data blocking when this is appropriate), as well as the evidence of the correct operation of these measures, which as has been said must be adapted to the ENS, could be used for this purpose.

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

Conclusions

Once the provision of the early childhood education service at the municipal kindergarten has been completed, the entity in charge of processing must return all personal information linked to the provision of this service to the City Council, given the principle of continuity of public services and the existence of legal provisions that require their conservation.

The assignment contract must establish the form and the term in which the person in charge must return the data to the person in charge. For the purpose of certifying the return, a document can be established through which the person in charge records the delivery of the data to the City Council, as well as, if applicable, that he has proceeded to the destruction of the copies and the total erasure of the existing data on your computer equipment, without prejudice to the pos

The person in charge can use any means at his disposal to prove the blocking of the data he keeps. Among others, it can use the documentation generated to implement the security measures related to the blocking of the data and the evidence of its correct operation.

Barcelona, August 24, 2020