CNS 50/2020

Opinion in relation to the query raised by a City Council in relation to the transfer of data to agents of the bodies and security forces without a written request for the investigation they carry out

A City Council consultation is presented to the Catalan Data Protection Authority in which the Authority's opinion is requested in relation to the communication of data to the Security Forces and Bodies (hereinafter, FFCCS), without the agents providing a written request for the investigation they are carrying out.

Having analyzed the request, in view of the current applicable regulations, and in accordance with the report of the Legal Counsel, the following is ruled.

I

(...)

II

The consultation explains that police officers would have requested from the City Council's public assistance office (OAC) *"a copy of the handwritten statements entered in the register by a specific person".*

According to the query, the police force justifies the request in the investigation of the commission of a crime by this person, and in order to check if she is the author of some writings, comparing her writing between these writings and an instance presented to the City Council. For this reason, according to the query, the agents request copies of the complete instances, including the sections where the personal data are recorded (name and surname, identity document, address, among others).

According to the query, the OAC would have required the agents if they can prove that they are carrying out said investigation in order to be able to justify the delivery of these documents. According to the consultation, the agents would have alleged that *"they do not need any accreditation, since they are acting within their powers."*

As a result of the assumption raised, and taking into account the applicable regulatory framework, the City Council makes the following inquiries:

"- If the City Council is obliged to provide information, personal data and copies of documents containing personal data to agents of the bodies and security forces without any written request of the investigation they are carrying out, apart from that the agents identify themselves to the municipal administration, in which the person or persons holding the data is involved or for whom they need access to certain information that may be contained in the municipal archives, with respect to certain procedures that have been managed before the administration municipal

- What could be, in this specific case, the possible consequences of providing information about a certain person that may contain personal data without being legally authorized to transfer it.

- In what cases is the City Council obliged to transfer personal data to the security forces and bodies, and what conditions must be met in order for this transfer to be legal."

It is necessary to start from the basis that not only the identifying data, such as the name and surname, the DNI or the address of a natural person that may appear in the information requested, but any other information that can be directly or indirectly related to the author of the writings to which you want to access, that may
stated in the requests that this person had submitted to the City Council register, are personal data (art. 4.1 of Regulation (EU) 2016/679, of April 27, general data protection (RGPD) and are protected by the regulations of
protection of personal data.

III

For expository purposes, we will first analyze the **third question** posed in the consultation: *"In which cases is the City Council obliged to transfer personal data to the bodies and security forces, and what conditions must be met in order for this transfer to be lawful"*.

The communication of personal information to the security forces and bodies constitutes a processing of personal data which, in the case of the City Council, is subject in the first place to the data protection regulations applicable to it, that is, the RGPD and the Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (LOPDGDD).

In accordance with these regulations, the City Council must comply, among others, with the principle of legality (art. 5.1.a) RGPD. Regarding the legality of the transfer of data referred to in the query, article 6 of the RGPD provides that:

"1. The treatment will only be lawful if at least one of the following conditions is met: a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes; (...).

c) the treatment is necessary for the ***fulfillment of a legal obligation***
applicable to the person in charge of the treatment;
(...)."

In the event that the consent of the affected person is not available (art. 6.1.a) RGPD), it will be necessary to take into account the relevant regulatory provisions, to analyze in which cases the communication of personal data included in the instances presented to
registration of the City Council in the FFCCS, can be considered sufficiently authorized for the purposes of article 6.1.c) RGPD. In other words, it is necessary to examine whether the City Council would have a "legal obligation" regarding the communication of data to the FFCCS, which would allow it to be considered that the legal basis of article 6.1.c) RGPD is met.

According to the consultation, the police force requesting the information would have alleged that the LECRIM, in articles 259, 262 and 264, *"regulates the circumstances in which it is mandatory to report a crime, under penalty of a fine. Therefore, data protection cannot be used to obstruct the reporting of a crime."*

However, this duty does not appear to be applicable in the case at hand.
The duty to report only applies when there is evidence or knowledge of the possible commission of a crime, a circumstance that does not seem to apply in the case at hand. For this reason, it does not seem that the reporting obligation provided for in the LECRIM can constitute in this case a legal obligation for the purposes of article 6.1.c) of the RGPD.

Having said that, for the purposes of the concurrence of the legal basis article 6.1.c) of the RGPD, it must be taken into account that according to the provisions of article 4.1 of Organic Law 2/1986, of March 13, of forces and security forces (LOFFCCS):

> *"1. Everyone has the duty to provide the Security Forces and Security Forces with the necessary assistance in the investigation and prosecution of crimes in the terms provided by law."*

The LOFFCCS thus establishes a general obligation of collaboration of any person, natural or legal, such as a City Council, with the FFCCS in relation to the investigation
and prosecution of crimes by them. For the relevant purposes, this provision could be considered as the legal obligation referred to in article 6.1.c)
RGPD, and which would allow a manager to communicate personal data in a lawful manner.

However, beyond the fact that the regulatory framework foresees this general obligation to collaborate with the FFCCS, and that this may translate into an obligation for the person in charge to communicate certain personal data (or other types of information), this does not implies that this is an absolute duty. In other words, it does not imply that the
responsible for the treatment, in this case the City Council, must communicate any information that is requested, nor that the communication must occur without the requirements of article 22.2 LOPD. It remains to be seen what information the police force is empowered to demand.

On this issue it should be borne in mind that the RGPD is not applicable to the treatments carried out by the security forces and bodies in the police and criminal judicial sphere, as can be seen from article 2.2.d) of the RGPD, which provides the following:

> *"2. This Regulation does not apply to the processing of personal data:*
>
> *(...)*
>
> *d) by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal sanctions, including protection against threats to public security and their prevention."*

In this area it is necessary to take into account Directive (EU) 2016/680 of the Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data by the authorities competent for the purposes of prevention, research, detection or prosecution of criminal offenses or the execution of criminal sanctions, and the free circulation of this data and by which the Framework Decision 2008/977/JAI of the Council is repealed.

The member states of the European Union had to transpose this directive before May 6, 2018.

In any case, given the lack of transposition of Directive 2016/680 by the Spanish State at the time of issuing this opinion, in the case at hand the provisions of Organic Law 15/1999 apply , of December 13, on the protection of personal data (LOPD), which remain temporarily in force in accordance with the fourth transitional provision of Organic Law 3/2018, of December 5, on the protection of Personal data and guarantee of digital rights (LOPDGDD), in relation to the information requests formulated by the FFCCS.

Therefore, to determine what information the police force is authorized to collect, it will be necessary to take into account article 22 of the LOPD, which enables the transfer of data for the fulfillment of *"police purposes".*

Thus, article 22.2 of the LOPD, provides the following:

> *"2. The collection and treatment for **police purposes** of personal data by the Security Forces and Bodies **without the consent of the persons affected** are limited to those cases and categories of data that are necessary for the **prevention of a real danger to public security or to the repression of criminal offences,** having to be stored in specific files established for that purpose, which must be classified by categories according to their degree of reliability."*

It will be necessary to assess the concurrence or not of this indeterminate legal concept in view of the circumstances of each case, and in relation to each request for information formulated by the FFCCS.

For its part, section 3 of article 22 LOPD establishes the following:

> *"3. The collection and processing by the Security Forces and Bodies of the data, to which the sections 2 and 3 of article 7 refer, may be carried out **exclusively** in the cases where it is **absolutely necessary for the purposes of a specific investigation,** without prejudice to the control of the legality of the administrative action or of the obligation to resolve the claims made in their case by the interested parties who correspond to the jurisdictional bodies.*

Thus, article 22.3 of the LOPD establishes a specific requirement for the transfer of data deserving of special protection (art. 7.2 and 7.3 LOPD) to the FFCCS, specifically, that this transfer is based and justified in the purposes of a specific investigation.

It cannot be ruled out that among the documents that the affected person may have presented to the City Council there is information that can be qualified as specially protected in accordance with articles 7.2 and 7.3 LOPD. But it is clear that taking into account that what the police are pursuing is not access to the content of the information contained in the writings, but only to be able to compare the handwriting, it would be clearly disproportionate to allow, for this purpose, access to information especially protected. The calligraphic samples provided should in any case refer to writings or fragments of writings that do not contain this type of information.

However, taking into account the information available, it does not appear that the query refers to the communication of data of special categories, so that it will be necessary to focus on the general provision of article 22.2 of the LOPD.

As this Authority has done on previous occasions (among others, the Opinions CNS 42/2014, CNS 47/2018, or CNS 28/2020, available on the website of

the Authority), article 22.2 of the LOPD could enable the transfer of certain data that are not data of specially protected categories (art. 7.2 and 3 LOPD) to the FFCCS for the prevention of a real danger to public security or for the repression of criminal offences, without the need to link this assignment to a specific investigation and without the need to necessarily link it to the performance of judicial police functions by the FFCCS (art. 126 Constitution; arts 574 and 149.1 of Organic Law 6/1985, of July 1, on the Judiciary (LOPJ), article 282 of the Criminal Procedure Law (LECRIM), and articles 2 and 4 of Royal Decree 769/ 1987, of June 19, of regulation of the judicial police).

In any case, in order for this transfer to be enabled, it will be necessary to comply with the requirements provided for in said article 22.2 of the LOPD, that is to say, that the data request is limited to those necessary for the prevention of a real danger to public safety or for the repression of criminal offences.

In the case in question, it seems that the police require the information for the repression of criminal offences, to the extent that it is indicated that it would be part of an investigation to verify the authorship of a certain document linked to the commission of one crime

If these requirements are met, or if any other qualifications apply in other rules with legal rank, the City Council should attend to the request for access to personal data formulated by the FFCCS.

IV

The consultation raises whether the City Council should communicate personal information *"without any* ***written request*** *of the investigation".*

On this issue, it should be borne in mind that the city council, as the person responsible for the treatment, is obliged to ensure the appropriate treatment of the information it has on its responsibility. Thus, article 5.2 RGPD establishes that *"The person responsible for the treatment will be responsible for complying with what is set out in section 1 and capable of demonstrating it* ***("proactive responsibility")."***

This will mean, in the case at hand, that the City Council, before communicating the data, must be able to verify both the identification of the person or persons making the request and compliance with the requirements to which the communication, in accordance with article 22 LOPD.

For these purposes, it should be taken into account at the outset that, with regard to police officers, Law 10/1994, of 11 July, of the Generalitat police - Mossos d'Esquadra, foresees that they must always prove their identity professional (art. 9.1). Identification that can be done through the TIP number.

Given the regulations studied, there would be no specific provision whereby, in general, any request for information by a police force must necessarily be submitted in writing. However, it should be remembered that, according to article 5.2 of the LOFFCCS in relation to the basic principles of action of FFCCS members:

"1 The following are basic principles of action for members of the Security Forces and Bodies: (...).

2. Relations with the community. Singularly:
(...).
b) (…). In all their interventions, they will provide complete information, and as wide as possible, about the causes and purpose of the same."

In any case, by application of article 22.2 LOPD, examined, it is up to the police force that requests information to prove and justify that the data it requests to know is necessary for the prevention of a real danger, or for repression of violations
penalties

This makes it necessary, at the outset, for a minimum justification on the part of the police force regarding the need to access certain personal data, in this case, for the repression of criminal offenses (given that, according to the query, the police force requests the information *"for the possible commission of a criminal act").*

v

Beyond what is set out in the previous legal basis, the City Council must not only ensure that the communication of certain data of the affected person has a sufficient legal basis and is lawful, but must be able to demonstrate that it has complied with the principles and its obligations derived from the data protection regulations before providing certain personal information of third parties.

Thus, the person in charge is bound, on the one hand, by the **principle of minimization,** according to which: *"Personal data will be: (...). adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("minimization of data");* (art. 5.1.c) RGPD).

Given the information available, the police force would have requested the "complete instances", including identification data of the person who submitted them to the register of the City Council, since *"they need to check if she is the author of some writings, comparing her writing between these writings and an instance presented to the city council."*

From the perspective of the minimization principle, that “instances completes" that a certain person submits to the City Council register, can affect personal information on matters of a very different nature (exercise of rights or obligations on the part of the affected party, claims, municipal procedures, etc.), including information of particular sensitivity, not only referring to the person presenting the instance, but to third parties, who may be referred to in any of the instances In the latter case, the access criteria should be even more restrictive.

In addition, the required instances could contain personal information of the affected person or of third parties, which are not merely identifying data, nor data deserving of special protection (art. 9 RGPD), but which are also unnecessary for the intended purpose which would be, based on the information available, to contrast the handwriting of the affected person with that contained in other documentation. Thus, for example, if the required instances contain professional data, bank data, data related to the family situation of the affected person, etc., it does not seem that their communication is necessary, at least for the purpose explained in the query.

According to the information provided in the inquiry, in principle it does not seem that in order to verify the authorship of some writings through a person's handwriting, access to the full content of an instance that is filed in the registry of a

City Council, which could contain more personal information than is strictly necessary, for the purposes of the minimization principle.

Therefore, and apart from the identification of the agents involved or the concurrence of a danger to public safety or the need for the justification of the communication for the need to suppress a criminal offence, in a case in which the request
of information is done as generically as in the case described in the consultation, so that the City Council can properly comply with the principle of minimization, it must be able to know if the police force considers it sufficient to limit communication to
identification data of the affected person or, otherwise, for what reason the "full instance" is required, or access to the various procedures that the affected person has been able to carry out before the City Council. Only in this way can you make the assessment relevant to the effects of the minimization principle.

In accordance with the principle of minimization, depending on the number of documents available from this person and their content, it would be necessary to assess the possibility of including in the response to the request documents or fragments of documents that do not include categories special data, or particularly sensitive, and the possibility of providing fragments of writings that, without revealing unnecessary information for the purposes of the request, allow the calligraphy check to be carried out.

In short, the City Council must be able to have enough information to carry out an analysis and assessment from the perspective of the minimization principle, to provide only the personal information that is necessary for the intended purpose, for which it is necessary for the police force to specify its request, and it is recommended that this specification be made in writing or through another means that allows us to record both the authorship and the specific scope of the request and its justification.

As this Authority has done in advance, in the face of any request for information made by the FFCCS that is not clear enough - either in relation to the specific functions performed by the police force requesting the information, either
in relation to the personal information that is specifically required -, the requested us
must be able to request clarification from the police force before communicating it.

Without clarification in writing about the reason and purpose of the request, about which personal data are requested (an instance that the affected person has presented to the City Council chosen at random, all the instances that he could have presented, etc. ...), on the need to access the "full" instance or the possibility of accessing fragments that do not contain relevant information, etc., it will be difficult for the City Council to check whether the communication conforms to the principles of protection of the aforementioned data, and if the requirements of article 22.2 of the LOPD, which we have referred to, are met.

In short, the City Council must be able to act diligently in the face of any request for personal information made by the police forces, and for this reason it must have the necessary information. In order to comply with the principle of proactive responsibility, the City Council should have a detailed written request from the police force.

For all that has been said, in relation to the **first question,** which refers to whether the City Council must provide the required personal information *"without any written request from the investigation",* although there is not in the studied regulations a express provision of the obligation so that the police force must formalize the request for information necessarily in writing, can be considered a requirement of the principle of proactive responsibility.

All this, without prejudice to the fact that, beyond the specific case examined, certain channels of communication can be established between the City Council and the FFCCS, which allow these types of information requests to be expedited or formalized and to provide a quick response, without distorting the necessary compliance with data protection principles by the City Council. The establishment of these communication channels - for example, through a computer application or through a call log with secure identification methods of the interlocutors of both bodies - would allow the City Council to be provided with the necessary information to to assess the relevance of the communication and thus comply with the principle of proactive responsibility.

VI

Finally, regarding the **second question** posed: *"What could they be, in this case specific case, the possible consequences of providing information about a certain person that may contain personal data without being legally authorized to transfer it",* we agree the following.

The City Council, as responsible, is subject to the sanctioning regime established in the data protection regulations (art. 82 et seq. RGPD, and art. 70 et seq. LOPDGDD).

As has been said, the City Council is responsible for complying with the principles of data protection (art. 5.1 RGPD), and must be able to demonstrate this compliance ("proactive responsibility" principle).

As has been pointed out, in principle, the communication of personal data in the terms and with the requirements provided for in article 22 of the LOPD, could have a sufficient legal basis for the purposes of the data protection regulations (art. 6.1 .c) RGPD), given the duty to provide the FFCCS with the necessary assistance for the investigation and prosecution of crimes (art. 4.1 LOFFCCS), which may involve the communication of personal data under the terms of article 22 LOPD.

However, the City Council must make sure that the communication is limited to relevant and suitable data for the intended purpose, and it must be able to demonstrate compliance with its obligations as the person responsible for the requested data. Otherwise, in the event that the City Council communicates personal data without the principles of data protection being complied with, this could constitute an infringement for breaching said principles (art. 83.5 RGPD).

In accordance with the considerations made so far, in relation to the consultation raised by the City Council, the following are made,

Conclusions

In the case analyzed, the City Council would be obliged to communicate the information that is relevant for the purposes provided for in article 22.2 LOPD when there is a real danger to public safety or the investigation and prosecution of crimes by the police forces .

Although there is no express provision in the studied regulations regarding the obligation to formalize the request for information necessarily in writing, it is justified that the request for information from the police force is made in writing, given the 'obligation that falls on the City Council to comply with the principle of proactive responsibility.

The communication of personal data without complying with the principles of data protection, may constitute an infringement due to violation of said principles (art. 83.5 RGPD).

Barcelona, February 4, 2021