CNS 43/2020

Opinion in relation to the consultation formulated by a city council on the creation of a supra-municipal network for the exchange of police information

A letter from the data protection delegate of a town hall is submitted to the Catalan Data Protection Authority in which it is requested that the Authority issue an opinion on the creation of a supra-municipal network for the exchange of police information

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 it is in its interest to create a network between local corporations that use the same police management computer program to share, between police forces, the information recorded in this program following the actions carried out by the local police .

It then details the following aspects of this information system:

1. When accessing the system, you must indicate the reason for the query:

• Requirement/judicial support. •
Prevention and public safety.

2. For each access, the identification of the user, the date and time of the access, the data consulted and the reason for the consultation will be recorded.

3. The information to be consulted/exchanged from the system will be as follows:

• Natural persons: first and last name; no. DNI/NIE/Passport or foreign document; sex; date of birth; place of birth; nationality; date of death (if applicable); aliases; name of father and mother; domicile/s; telephone/s; email/s; creation/modification date of the record; module of the management program with which the person is related (daily news, traffic accident, certificate, court summons, etc.).

• Legal persons: commercial name; CIF; activity; domicile/s; telephone/s; email/s; contact person/s data; creation/modification date of the record; module of the management program with which the entity or company is related.

• Vehicles: registration; Mark; model; rack; type of vehicle; insurance; data of the owner; module of the management program with which it is related.

- **Ownership of animals: microchip; microchip type; name of the animal; animal species; race; dangerousness; date of birth; date of death (if applicable); data of the owner.**

The City Council states that it has formalized with the company that owns the police management computer program the corresponding data controller contract. Also that a risk analysis is being carried out and that it is planned, if necessary, to carry out an impact assessment.

In addition to all this, it raises whether the system of access, consultation and exchange of information for local corporations that voluntarily adhere to this police information system, in the terms set out, complies with the current regulations on data protection personal

III

In order to respond to the query made, it is necessary to analyze, at the outset, what the applicable data protection regulations would be.

Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data and by which Directive 95/46/CE (RGPD) is repealed, it is not applicable to the treatments that are carried out in the police and criminal justice field, as can be seen from article 2.2.d) of the RGPD, which provides the next:

> **"2. This Regulation does not apply to the treatment of personal data: (...)**
> **d) on the part of the competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal sanctions, including that of protection in the face of threats to public security and their prevention."**

In this area it is necessary to take into consideration Directive (EU) 2016/680 of the Parliament and of the Council, of April 27, 2016, relating to 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/JA

EU member states had to transpose Directive (EU) 2016/680 by May 6, 2018.

Given the lack of transposition of this Directive by Spain, in the case at hand it is necessary to take into account the provisions of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (LOPDGGD), which in the fourth transitional provision establishes the following:

> **"The treatments subject to Directive (EU) 2016/680 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of individuals with regard to the treatment of personal data by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, and the free circulation of said data and by which the Framework Decision 2008/977/JAI of the Council is repealed, will continue to be governed by the Organic Law 15/1999, of December 13, and in particular article 22, and its development provisions, as long as the rule that transposes the provisions of the said directive into Spanish law does not enter into force.**

Therefore, in this case it is necessary to bear in mind the provisions of Organic Law 15/1999, of 13 December, on the protection of personal data (LOPD) and the provisions that implement it.

IV

The consultation considers the possible creation of a supra-municipal police information system that would allow the police force of local corporations that voluntarily join to consult and, therefore, exchange information of police interest.

In this system, for the information that is available, the information available to each local police will be incorporated as a result of the exercise of their functions (both as a result of planned services and at the request of citizens), which it includes personal data, and which the police force manages through a computer program called DRAG, created by a private company.

Beyond that, the role of the different agents involved in this information system is not clear in the consultation. In any case, and in the absence of more precise information about the model to be adopted, the intended purpose could be achieved through several alternative organizational models.

In accordance with article 3.d) of the LOPD, "responsible for the file or treatment" is understood to be the "physical or legal person, of a public or private nature, or an administrative body, which decides on the purpose, content and use of the treatment".

In the consultation, it is noted that the City Council "is interested in creating a network between local corporations that use the same DRAG program", a manifestation of which it could be deduced that this local corporation assumes the position of responsible for the information system and , therefore, responsible for the treatment.

Nor could it be ruled out, however, that we are faced with an assumption of joint responsibility, that is, that the different local corporations that have this police information management computer program (DRAG) agree and participate together in the creation of the new information system police, therefore, in the definition of the ends and means of the treatment.

Although the term co-responsible for the treatment is not expressly defined in the LOPD, it is referred to in article 5.1.q) of the Regulations for the deployment of the LOPD, approved by Royal Decree 1720/2007, of December 21 (RLOPD), in defining the person responsible for the treatment as "the natural or legal person, of a public or private nature, or an administrative body, that alone or jointly with others decides on the purpose, content and use of the treatment, although not I realized it materially.".

In any case, this figure is included in Directive 2016/680, which must be transposed into the Spanish legal system.

Article 21 of the Directive provides that:

> **"1. The Member States will provide that, when two or more persons responsible for the treatment jointly determine the objectives and the means of treatment, they are considered co-responsible for the treatment. They will determine, transparently and by mutual agreement, what will be their respective responsibilities in compliance with this Directive, in particular with regard to the exercise of the rights of the interested party and their respective obligations in the supply of the**

information contemplated in article 13, except and to the extent that the respective responsibilities of those responsible are governed by the Law of the Union or the Member State to which those responsible for the treatment are subject. The aforementioned agreement will designate the point of contact for those interested. Member States may designate which of the co-responsible persons can act as a single point of contact for the interested party regarding the exercise of their rights. 2. Regardless of the terms of the agreement referred to in paragraph 1, the Member States may provide that the interested party can exercise the rights recognized by the provisions adopted in accordance with this Directive with respect to each of those responsible and to it."

Therefore, if the present case is a case of co-responsibility, it would be advisable to take into account what is established in this precept, without prejudice to what may be established in the future transposition rule.

Be that as it may, warn that the responsibility in these cases would cover only the police information incorporated in the new information system, not so the information available to each local corporation in the respective police management information systems. In this case, each local police would be responsible for the treatment of the information generated by their actions, without prejudice to the fact that, once incorporated into the new system, it would become part of the responsibility of the consulting City Council (or, as the case may be , of the set of participating local bodies (case of co-responsibles)).

With regard to the company that created the DRAG police management computer program, in the consultation it is pointed out that it has the corresponding treatment commission contract, which includes "contractual clauses with the general contents of the legal regime of the "order and the specific contents of this type of processing order".

Therefore, in the present case, said company would hold the status of data controller (article 3.g) LOPD), understood as "the natural or legal person, public authority, service or any other body that, alone or jointly with others, treat personal data for the account of the person responsible for the treatment".

Beyond the fact that this processing contract must comply with the provisions of article 12 of the LOPD, until the rule that transposes Directive 2016/680 into Spanish law comes into force, it is recommended to have also taking into account what is established in article 22 of this Directive.

A third possibility could be that we are faced with a decentralized organizational model. In this case, each local corporation would be responsible for the treatment of the information generated by its actions and managed through the DRAG computer program, and the proposed information system would only be a mechanism or means to facilitate the transmission of the information that at a given moment a local police force may require another local police force to carry out their duties.

In any case, the definition of what is the role of the different administrations involved, a decision that must be taken by the entities involved, becomes an essential element to determine the obligations and responsibilities that may correspond to each of the administrations involved.

v

Having said that, both the creation of this police information system and the information flows that occur from its implementation must be placed within the regulatory framework

applicable to the actions of the local police, in order to consider them legitimate from the point of view of the protection of personal data.

According to the LOPD, the creation of police files, as well as the processing and communication of their data, is restricted to the public administrations that have powers attributed to public security (articles 22), including , the local corporations.

In this sense, Organic Law 2/1986, of March 13, regulating the Forces and Bodies of State Security (LOFCSE), provides that:

> **"First article**
> **1. Public Security is the exclusive competence of the State. Its maintenance corresponds to the Government of the Nation.**
> **2. The Autonomous Communities will participate in the maintenance of Public Security in the terms established by the respective Statutes and within the framework of this Law.**
> **3. The Local Corporations will participate in the maintenance of public security in the terms established in the Law Regulating the Bases of Local Government and in the framework of this Law.**
> **4. The maintenance of Public Security will be exercised by the different Public Administrations through the Security Forces and Bodies."**

The LOFCSE regulates in general terms the local police (Title V) and considers them as another security force alongside the state and regional police (Article 2). It also specifies common functions for all Security Forces and Bodies (article 11).

Law 16/1991, of 10 July, on local police (LPL) incorporates this set of functions in its legal text.

Thus, in accordance with article 11 of the LPL, the following functions correspond to the local police that depend on the municipalities of Catalonia, in their scope of action:

> **"a) To protect the authorities of the local corporations and to watch and guard the buildings, installations and dependencies of these corporations. b) Order, signal and direct traffic in the urban core, in accordance with what is established by the traffic rules. c) Instruct attestations for traffic accidents that have occurred within the urban core, in which case they must communicate the actions taken to the competent security forces or bodies. d) Act as administrative police, in order to ensure compliance with regulations, ordinances, bans, resolutions and other municipal provisions and acts, in accordance with current regulations. e) Act as judicial police, in accordance with article 12 and current regulations. f) Carry out preventive measures and actions aimed at preventing the commission of criminal acts, in which case they must communicate the actions carried out to the competent security forces or bodies. g) Collaborate with the forces or security forces of the State and with the Autonomous Police in the protection of demonstrations and in the maintenance of order in large human concentrations when they are required to do so. h) Cooperate in the resolution of private conflicts, when required to do so. i) Monitor public spaces. j) Provide assistance in accidents, catastrophes and public calamities, participating, in accordance with the provisions of the laws, in the execution of civil protection plans.**

k) Ensure compliance with current environmental and environmental protection regulations. l) Carry out actions intended to guarantee road safety in the municipality. m) Any other police and security function that, in accordance with current legislation, is entrusted to them."

Therefore, the local police of the town councils (with the designation of local police, municipal police, urban guard or other traditional ones) remain legitimate to carry out the processing of personal data that they require for the exercise of the legally entrusted functions.

With regard specifically to the possibility of sharing this type of information, it should be borne in mind that the applicable legislation foresees an obligation of collaboration between the State Security Forces and Bodies for the exercise and development of the set of functions they are assigned, which also includes the duty to communicate information that may be relevant and necessary for that purpose.

On this matter, the LOFCSE provides that "the members of the Security Forces and Cuerpos will adjust their actions to the principle of reciprocal cooperation and their coordination will be carried out through the bodies established for this purpose by this Law" (article 3).

Also that "the members of the Security Forces and Bodies of the State and of the Police Bodies of the Autonomous Communities must provide mutual assistance and reciprocal information in the exercise of their respective functions" (article 45 LOFCSE).

In accordance with Law 4/2003, of April 7, on the organization of the public security system of Catalonia, the police of the Generalitat-mossos d'esquadra and the police of the councils constitute the police of the institutions of Catalonia (article 5).

This same Law 4/2003 regulates the principles to which the public administrations with powers on security must adhere, among which the one of "reciprocal information, especially when necessary to better fulfill the powers of each administration" stands out (article 21.b)).

In this sense, the Law provides that "the authorities and members of the police force of the Generalitat-mossos d'esquadra and the local police forces of Catalonia are obliged to provide each other with information that is relevant for compliance of the respective functions, without prejudice to the reservation that is appropriate for the reason of the matter and with full respect of the applicable legislation, in particular that relating to the protection of personal data" (article 23.1 Law 4/2003).

It should also be borne in mind that the LOPD itself legitimizes the communications of personal data that take place between public administrations when these have as their purpose the exercise of identical powers or that refer to the same matter.

Specifically, article 21.1 of the LOPD establishes that "personal data collected or processed by public administrations for the exercise of their powers must not be communicated to other public administrations for the exercise of different competences or competences when they deal with different subjects, except when the purpose of the communication is the subsequent processing of the data for historical, statistical or scientific purposes". Section 4 of the same article states that "in these cases the consent of the affected person is not necessary".

In this sense, article 10.4.c) of the RLOPD complements the legal regulation pointing out that the consent of the interested party will not be necessary when the transfer between administration

public works are carried out "for the exercise of identical powers or relating to the same subjects".

Point out that, in order to facilitate the exchange of information between police forces, Law 4/2003 foresees that the department with powers in matters of public security must manage and maintain a unified system of police information, to which the Mossos d'Esquadra body and the local police of Catalonia have access, the same Law providing that through a bilateral adhesion agreement the conditions of access and participation of each local police body are regulated (article 24.2).

Also that the Mossos d'Esquadra body must facilitate local police access to other databases, in cases of local interest that are determined by regulation (article 24.3 Law 4/2003).

And, with regard to the IT program implemented by the Mossos d'Esquadra body, which by means of an agreement it has been foreseen that the local police can use it, as well as the work in integrated networks of police information (article 24.4 Law 4/2003).

In the consultation it is pointed out that the information system that is intended to be created "does not interfere with the processing of information between police officers by means of the SIP or other shared information systems", this is the unified information system police referred to in the aforementioned provisions of Law 4/2003.

It is, it is argued in the consultation, a "complementary system and in no case will the necessary or mandatory information be uploaded or shared in the SIP to be able to carry out the police functions and tasks regulated by the laws."

It should be noted, at this point, that Law 4/2003 provides that "the Government, through the department in charge of public security, has the responsibility to make effective the coordination of the local police, which involves the determination of the means and systems of relationship that make possible the joint action of these bodies, through the competent authorities, so that the integration of the respective particular actions is achieved within the whole of the security system that is entrusted to them" (article 25.1).

The LPL also provides that "for the purposes of this Law, "coordination" means the determination of the means and the relationship systems that make possible the joint action of the local police, through the competent authorities, so that achieve the integration of the respective particular actions within the overall public security system that is entrusted to them" (article 14).

On this issue, article 15 of the LPL specifies that:

> **"1. The coordination of the activity of the local police can be extended, in any case, to the following functions: a) Promote the homogenization of the technical means and the uniformity of the other elements common**
>
> **b) Establish the instruments and means that make possible a reciprocal information system. (...).”**

Given this, although it could be said that, from the data protection side, there would be sufficient legal cover for the exchange, between local police forces, of that personal information that may be of interest to the exercise of the functions that are legally attributed to them, the creation of an information system like the one proposed in the consultation seems to require th

intervention of the department competent in matters of public security of the Administration of the Generalitat.

In any case, note that, from the point of view of the protection of personal data, it is necessary to ensure that any of these communications of police information, apart from having sufficient legitimacy, are appropriate, among others , to the principle of data quality (article 4 LOPD).

This principle, in its aspect of limiting the purpose and minimization of data, requires that personal data must be collected for specific, explicit and legitimate purposes, their subsequent treatment being incompatible with these purposes, and they must be adequate, relevant and limited to what is necessary to achieve these purposes to justify their treatment.

It must be taken into consideration, therefore, that the accesses or communications of data that take place following the implementation of this information system can only be considered adequate to the data protection regulations to the extent that they are limited to the data personal data that each local police force requires for the exercise of the functions that, in accordance with the applicable legislation, are within their competence, and provided that this data is necessary, relevant and appropriate in each case.

This same principle, in its aspect of data accuracy, also requires that personal data be accurate and updated so that they respond truthfully to the current situation of the affected person. For this reason, it is also necessary to foresee mechanisms that guarantee the quality of the personal information incorporated in the police information system, in such a way that the data that is treated is accurate and updated at all times, a matter that could be made difficult if the coexistence of parallel information systems with matching objectives, even if only partially.

VI

On the other hand, with regard to the implementation of the information system, the need to adopt the necessary technical and organizational measures that guarantee the security of the data and avoid its alteration, loss, treatment or unauthorized access, taking into account the state of technology, the nature of the data stored and the risks to which they are exposed, whether they come from human action or the physical or natural environm

On this issue, remember that the new European regulatory framework for the right to the protection of personal data (both Directive 2016/680 and the RGPD) sets up a security system that is based on determining, following a prior risk assessment , which technical and organizational measures must be applied to guarantee security levels appropriate to the risk in ea

This new model is based on the principle of proactive responsibility so that not only must the rule be complied with, but also must be able to demonstrate it, and on data protection by design and by default, in such a way that both at the time of defining the different processing operations, and at the time of determining and applying the means that will be used to process personal data, the principles, rights and obligations that includes the personal data protection regulations that apply to the treatments that are intended to be carried out.

Therefore, it is necessary to carry out this risk analysis prior to putting the information system into operation to determine the appropriate technical and organizational security measures to safeguard the right to data protection of possible

affected

Point out, in relation to the determination of these measures, that the scheme of security measures provided for in the RLOPD, although compliance would be mandatory at this time, might not be sufficient once Directive 2016/680 is transposed . In some cases this scheme can continue to be applied, if the previous risk analysis concludes that the measures are really the most appropriate to offer a level of security suitable for the specific case, but in others it may be necessary to complete them with additional measures resulting fr

In the query, there is express reference to the implementation of an access register, so that, for each access, it is planned to record the name of the system user, the day and time of access, the data consulted and the reason for the consultation.

Beyond positively assessing the implementation of this security measure, the need to evaluate the adoption of other additional measures, such as the establishment of appropriate mechanisms that allow the correct identification and authentication of system users of information for the purposes of guaranteeing that unauthorized treatments will not occur, among others.

It should be borne in mind, given article 29.2 of Directive 2016/680 (pending the transposition rule), that the security measures to be implemented in a case such as the one being examined should be addressed in all case to:

> **"a) deny access to unauthorized persons to the equipment used for the treatment (control of access to the equipment); b) prevent the data supports from being read, copied, modified or canceled by unauthorized persons (control of the data supports); c) prevent stored personal data from being entered without authorization, or from being inspected, modified or deleted without authorization (storage control); d) prevent automated processing systems from being used by unauthorized persons through data transmission facilities (user control); e) guarantee that the persons authorized to use an automated processing system can only have access to personal data for those who have been authorized (data access control); f) guarantee that it is possible to verify and establish to which organizations they have been transmitted or can be transmitted or to whose disposal personal data can be put through data communication equipment (transmission control); g) guarantee that it can be verified and confirmed afterwards which personal data have been entered into the automated processing systems and at what time and by which person they have been entered (control of the introduction); h) prevent personal data from being read, copied, modified or deleted without authorization during the transfer of personal data or during the transport of data carriers (transport control); i) guarantee that the installed systems can be restored in case of interruption (restoration); j) guarantee that the functions of the system do not present defects, that operating errors are signaled (reliability) and that the stored personal data are not degraded by system malfunctions (integrity)."**

Also, it must be said, it would be necessary to adopt and implement training measures for the staff who must process the personal data in question.

In any case, agree that these security measures should conform to the National Security Scheme (article 1 Royal Decree 3/2010, of January 8).

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

Conclusions

It is necessary to define the responsibilities of the different agents involved in the implementation of this information system to determine the obligations and responsibilities of each of them.

There is authorization for the exchange of information between the different police forces, always in accordance with the coordination made by the competent Department in the matter of local police, but it is necessary to respect the principle of data quality, the principle of accuracy and, after risk analysis, determine the appropriate security measures to guarantee the rights of the people affected.

Barcelona, November 30, 2020