Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

In this resolution, the mentions of the affected population have been hidden in order to comply with art. 17.2 of Law 32/2010, given that in case of revealing the name of the affected population, the physical persons affected could also be identified.

File identification

Resolution of sanctioning procedure no. PS 45/2019, referring to the City Council of (...).

Background

1. On 16/01/2019, the Catalan Data Protection Authority received a letter from a person filing a complaint against the City Council of (...), on the grounds of an alleged non-compliance of the regulations on personal data protection. In particular, the complainant stated that two agents of the Urban Guard of (...) had made several accesses to the police information systems which, in appearance, would not have been justified in the exercise of their duties. These possibly improper accesses would have been noted following an audit (no. (...)) carried out by the Information Systems Division
Police officer of the Police of the Generalitat-Mossos d'Esquadra (hereafter, PG-ME). Among the people affected by these accesses, there would be people employed by the City Council, people linked to them, members of the local Corporation (current and previous), as well as members of various political parties and local business people. The reporting person provided various documentation about the events reported.

2. The Authority opened a preliminary information phase (no. IP 17/2019), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. In this information phase, on 18/01/2019 the reported entity was required to report, among others, on whether any action had been taken to check whether access to the systems of police information carried out by the agents of the Urban Guard to which the aforementioned audit referred, were justified in the exercise of their functions; as well as whether disciplinary actions had been initiated.

4. On 31/01/2019, the City Council of (...) responded to the above-mentioned request through a letter in which it stated, among others, the following:

- That, on 27/12/2018, the Chief of Police of (...) presented a letter highlighting the existence of serious facts that could constitute a very serious disciplinary offence.
- That on 01/21/2019 the City Council had full access to the audit carried out by the PG–me

- That, in view of that information, the City Council saw the need to process the respective disciplinary procedures, requesting collaboration from the General Sub-Directorate for Coordination of the Police of Catalonia.

5. On 14/11/2019, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the City Council of (...), firstly, for an alleged infringement provided for in article 83.5.a), in relation to article 6; and, secondly, for an alleged violation provided for in article 83.4.a), in relation to article 33; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 11/22/2019.

6. On 16/12/2019, the City Council of (...) made objections to the initiation agreement.

7. On 20/01/2020, the person instructing this procedure formulated a proposed resolution, by which he proposed that the director of the Catalan Data Protection Authority admonish the City Council of (...) as responsible, in the first place, for an infringement provided for in article 83.5.a) in relation to article 5.1.f); and secondly, of an infringement provided for in article 83.4.a) in relation to article 33, all of them of the RGPD.

This resolution proposal was notified on 20/01/2020 and a period of 10 days was granted to formulate allegations.

8. The deadline has been exceeded and no objections have been submitted.

proven facts

Of all the actions taken in this procedure, the facts detailed below are considered accredited.

1. Between 10/08/2017 and 29/11/2018, agents (...) and (...) of the Urban Guard of (...) accessed the Police Information System - SIP – (both in the SIP for natural persons and in the SIP for vehicles), to consult information related to the chief inspector of the Urban Guard of (...) and his family (including his ex-partner); to people who were or had been councilors of the City Council of (...); to people connected with the Candidature of Popular Unity, with Initiative for Green Catalonia and with the Partit dels Socialistes de Catalunya; to business people from (...); to agents of the Guardia Urbana; and civic agents from (...).

These accesses were not justified in the exercise of their functions.

2. The City Council of (...), and in particular, the chief inspector of the Urban Guard became aware of the above facts, at least, on 24/12/2018 (the date on which he maintained a conversation with the mayor in relation to these facts). Later, by email

dated 12/27/2018 addressed to the mayor and the competent councilor, the inspector attached the "Proposal of disciplinary file 27 12 2018" related to the aforementioned facts.

The City Council of (...) did not notify the Authority of this security breach.

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. The accused entity has not made allegations in the resolution proposal, but it did so in the initiation agreement. Regarding this, it is considered appropriate to reiterate below the most relevant part of the motivated response of the instructing person to these allegations.

As indicated by the instructing person in the resolution proposal, in the statement of objections to the initiation agreement, the City Council of (...) did not question any of the facts imputed in the present sanctioning procedure .

Indeed, regarding the unauthorized access to the SIP by the two previously identified agents (proved fact 1 of this proposal), the City Council reported that "he has instituted several disciplinary proceedings to clear possible responsibilities, to correct possible conduct infringing acts, so that they are avoided in the future and to know their maximum possible dimension the scope of possible infringing conduct, which currently is in find processing."

And regarding the lack of notification of the security breach (proven fact 2 of this proposal), the City Council stated that "it is the disposition of the APDCAT to provide any information, requested at any time, regarding the possible security violation that was generated." in a

Given the above, the City Council requested in its statement of objections to the initiation agreement that the present sanctioning procedure be dismissed.

Well, as the instructing person explained in the resolution proposal, it must be made clear that neither the initiation of disciplinary actions against the agents of the Guard of (...) related to the events reported; nor the offer to provide information on the security breach, if the Authority requires it, do not allow the imputed facts to be distorted, nor their legal qualification.

Despite the above, it is considered appropriate to highlight the City Council's diligence in initiating disciplinary actions against people who unjustifiably accessed certain information contained in the SIP without being justified in the exercise of their duties functions This circumstance must mean that it becomes unnecessary to propose to the City Council the initiation of disciplinary actions as provided for in article 46.2 of Organic Law 15/1999, of December 13, on the protection of personal data (LOPD), in effect at the time the said improper accesses were consummated.

In turn, it is also necessary to positively assess the attitude shown by the Consistory to assist the Authority when it requires it.

3. In relation to the facts described in the first point of the proven facts section, relating to the principle of confidentiality, it is necessary to go to article 5.1.f) of the RGPD, which regulates it determined that personal data will be "treated in such a way that they are guarantees an adequate security of the unauthorized personal, including the protection against its loss, destruction or accidental damage, through the appropriate no unauthorized or illegal treatment and against technical measures or organizations". or application u

In the present case, between 10/08/2017 and 29/11/2018, two agents of the Urban Guard accessed the SIP to consult information linked to several people, without this being necessary for the exercise of their duties functions, which is why it is considered that the confidentiality of this data was violated.

As indicated by the person instructing, during the processing of this procedure the facts described in point 1 of the proven facts section, which are considered constitutive of the offense provided for in article 83.5.a) of the RGPD, which typifies the violation of which includes the principle of integrity and "the basic principles for treatment(...)" , confidentiality

4. With regard to the fact described in point 2 of the proven facts section, it is necessary to refer to article 33.1 of the RGPD, which provides that "In violation of the security of personal data, the treatment will notify the competent control authority responsible for the in accordance with article 55 without undue delay and at the latest 72 hours after of the security risk for the rights and liberties of individuals. unless it is improbable that said violation if possible, have had evidence of it, constitute a the control authority a one takes place within 72 hours, it must be accompanied by an If the notification no indication of the reasons for the delay."

In the present case, the City Council of (...), and specifically, the chief inspector of the Urban Guard became aware of the improper access to the SIP, at least, on 24/12/2018 (date in which he held a conversation with the mayor in relation to these facts), based on the information contained in the two audits carried out by the Police of the Generalitat-Mossos d'Esquadra in relation to access to the SIP (the report of the first audit was communicated to the City Council on 11/12/2018).

In accordance with what has been set forth, as indicated by the instructing person, the fact contained in point 2 of the proven facts section, relating to the lack of notification of the security breach, constitutes the violation provided for in article 83.4.a) of the RGPD, which typifies the violation of "the obligations of the responsible person in charge and tenor of articles 8, 11, 25 aa 39, 42 43"y , among which is the obligation to notify the Authority of personal data security violations within 72 hours of becoming aware of them.

The conduct addressed here (which took place when the LOPDGDD was already in force) has been included as a serious infringement in article 73.r) of the LOPDGDD, in the following form:

> r) Failure to comply with the duty to notify the data protection authority of a personal data security breach in accordance with the provisions of article 33 of Regulation (EU) 2016/679."

5. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

> "(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the behavior ceases or the effects of the infringement that has been committed are corrected.
> The resolution has to notify the person in charge or the treatment, the body on which it depends hierarchically, if applicable, and those affected who have the status of interested party, if applicable."

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010, determines the following:

> "2. In the case of offenses committed in relation to files of public ownership, the Director General of the Catalan Data Protection Authority [illegible], persons, if any". adopt for the initiation of actions

In this same sense, article 46 of the LOPD (valid until the entry into force of the LOPDGDD), applicable in relation to the 1st of the proven facts of this proposal, provided that in the case of offenses committed by the public administrations, in the resolution in which the infringement is declared, the measures to cease or correct the effects of the infringement shall be established, if applicable; as well as proposing the initiation of disciplinary actions, if appropriate.

As has been advanced, the City Council of (...) reported that it had initiated disciplinary "various" proceedings to clear the responsibilities arising from the proven fact 1 of this proposal. Given the above, it is unnecessary to propose the initiation of disciplinary actions in the present case.

On the other hand, as explained by the investigating person in the resolution proposal, no request for measures to correct the effects of the imputed infringements should be proposed, given that these derive from facts that have already been accomplished.

resolution

For all this, I resolve:

1. Admonish the City Council of (...) as responsible, in the first place, for an infringement provided for in article 83.5.a) in relation to article 5.1.f); and secondly, of an infringement provided for in article 83.4.a) in relation to article 33, all of them of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 5th legal basis.

2. Notify this resolution to the City Council of (...).

3. Communicate the resolution issued to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

4. Order that this resolution be published on the Authority's website (apdcat.gencat.cat), in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with the provisions of article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

The director,