Carrer Rosselló, 214, esc. A, 1st 1st
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

Archive resolution of the previous information no. IP 342/2020, referring to the City Council of (...).

Background

1. On 13/11/2020, the Catalan Data Protection Authority received a letter from a person (an agent of the Urban Guard of (...) -hereinafter, GU-) in which he formulated a complaint against the City Council of (...), due to an alleged breach of the regulations on the protection of personal data.

First of all, the complainant stated that on 12/12/2018, the head of the GU asked the Division of Police Information Systems (hereinafter, DSIP) of the General Directorate of the Police (hereinafter, DGP) of the Department of the Interior, an audit
of access to police information systems (hereinafter, SIP) without complying with the minimum legal requirements (according to the reporting person: real motivation for requesting it, purpose pursued and motivation for specifying the period to be audited).

The complainant added that, according to the report drawn up by the head of the GU, 12,500 inquiries were verified in the SIP, but the report only referred to about 40 inquiries (0.2% of total).

The reporting person also requested to know through which channel the audited data was sent and who received it and where; what has been done with the rest of the data; as well as
for what reason have they been rejected and under what criteria.

2. The Authority opened a preliminary information phase (No. IP 342/2020), 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 were capable of motivating the initiation of a sanctioning procedure.

3. In the framework of this preliminary information phase and the one initiated following the complaint by another person against the City Council of (...) (IP 333/2020) related to the same facts, on date 03 /03/2021 said entity was required to provide the risk analysis to determine the measures to guarantee the security of the City Council's systems of the data consulted in the SIP; as well as if the information linked to the queries that is not

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

considered illegal (that is, those that were not the subject of disciplinary proceedings), had been deleted or blocked.

4. On 04/08/2021, the City Council of (...) responded to the aforementioned request through a letter in which it stated, among others, the following:

- That after consulting the GU and the departments of the City Council that could have evidence of the demand for a risk analysis in relation to the consultations carried out in the SIP, the existence of the same is unknown.
- That after consulting the services involved, it was not stated that any data had been deleted or blocked from any municipal or supra-municipal records in relation to inquiries made.

Fundamentals of law

1. In accordance with the provisions of articles 90.1 of the LPAC and 2 of Decree 278/1993, in relation to article 5 of Law 32/2010, of October 1, of the Authority Catalan Data Protection Agency, and article 15 of Decree 48/2003, of February 20, which approves the Statute of the Catalan Data Protection Agency, the director of the Catalan Data Protection Authority.

2. Based on the background story, it is necessary to analyze the facts reported that are the subject of this file resolution.

2.1. About the audit requirements.

The complainant stated that, on 12/12/2018, the head of the GU asked the DSIP for an audit of the accesses to the SIP (performed by him and another agent of the GU) without complying with the minimum legal requirements, which according to the reporting person would be the real motivation for requesting it, the purpose pursued and the motivation for the concretization of the period to be audited.

It should be noted that the reporting person did not provide the audit request that the head of the GU would have formulated on 12/12/2018; nor did it specify the rule that would include said legal requirements that, according to the complainant, the audit requests should fulfill.

Having said that, it should be emphasized that the audit or access registration is a security measure aimed at verifying that the accesses to the information system have been carried out in the exercise of the functions entrusted to the people users who access it.

Article 5.1.f) of 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

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

to the free circulation of these (hereinafter, RGPD) contemplates the principle of integrity which implies that personal data must be treated in such a way as to guarantee adequate security, including protection against unauthorized treatment or unlawful and against the loss, destruction or accidental damage of data, through appropriate technical or organizational measures.

For its part, article 32.1.d) of the RGPD provides that the data controller must implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, which if applicable includes a process to verify , evaluate and regularly evaluate the effectiveness of the technical and organizational measures established to guarantee the safety of the treatment. And the 4th paragraph of article 32 of the RGPD also determines that the person in charge must adopt measures to ensure that any person acting under his authority and who has access to personal data can only process this data following the instructions of the responsible, unless obliged to do so by virtue of the law of the Union or the Member States.

Given that the DGP of the Department of the Interior is responsible for the SIP, it is up to her (through the DSIP) to carry out the audits on access to this police information system.

Well, the request for said audit by the head of the GU was based on the fulfillment of a legal obligation in accordance with articles 6.1.c), 5.1.f) and 32 of the RGPD, as well as in the fulfillment of a mission carried out in the public interest or the exercise of public powers in accordance with article 6.1.e) of the RGPD and Law 16/1991.

In turn, the conduct of the audit by the DSIP (DGP) would also be based on the same legal bases. Therefore, these treatments are lawful.

So, regardless of the content of the request made by the head of the GU (who must be considered to be an authorized person to request an audit on access to the SIP) on 12/12/2018 (which the complainant does not provide), to whom the final decision to prepare a audit is to the person in charge of the treatment, that is to say to the DSIP.

In any case, it must be reiterated that this audit must be understood as a security measure that allows any query made to the SIP to be verified at any time; as well as the purpose pursued is to guarantee the security of the data included in said information system.

2.2. About the 12,500 audited queries.

The person making the complaint pointed out that in the report drawn up by the head of the GU (it is inferred that it refers to the report issued on 01/02/2019) it is made clear that

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

they verified 12,500 SIP inquiries (made by the complainant and another officer), but that the report only picked up about 40 (0.2% of the total).

Well, this circumstance is irrelevant, to the extent that all accesses made by users to an information system can be audited.
More so considering the nature of the SIP.

No breach of data protection regulations is observed, due to the fact that the aforementioned report did not include information relating to the audited SIP queries and that should not have been considered illegal. In fact, this would conform to the principle of data minimization (art. 5.1.c RGPD), according to which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which are treated

Having said that, although it was not expressly denounced, it should be pointed out that as of today, the Director of the Authority has agreed to initiate disciplinary proceedings against the City Council of (...) for not certifying that it has carried out an analysis of risks to determine the appropriate technical and organizational measures to ensure the security of personal data that are processed within the framework of disciplinary procedures, such as

linked to the 12,500 controversial SIP inquiries.

Linked to this, the reporting person requested to know what had been done with the rest of the data (the queries to the SIP audited and which would not have been considered illegal).

This matter must be understood as referring to the conservation of the rest of the data linked to the audited SIP consultations and which would not have been the subject of the disciplinary procedure imposed on the person making the complaint here and on another agent.

In this regard, it is appropriate to refer to article 5.1.e) of the RGPD, which regulates the principle of limitation of the retention period determining that personal data must be kept in such a way as to allow the identification of the interested parties for a period no longer than necessary for the purposes of treatment. And it adds that personal data can be kept for longer periods, as long as they are treated exclusively for archival purposes in the public interest, among others.

Well, without prejudice to the fact that said consultations with the SIP could continue to be necessary to achieve the intended purpose, it is inferred that in the present case these data collected during the actions prior to the start of the disciplinary procedures should be kept for archive in the public interest.

In this regard, it should be noted that the document evaluation and access table with code 751, relating to the documentary series "Very serious disciplinary proceedings in personnel matters" (in the present case, the infractions were classified as very serious), contemplates the permanent conservation, which would also affect the information collected both in the

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

within the framework of the disciplinary procedures themselves, as in the previous actions carried out prior to the start of the procedure.

2.3. On other issues raised by the complainant.

Subsequently, the complainant requested to know through which channel the audited data was sent and who received it and where.

The reporting person does not report any conduct contrary to the regulations on data protection, but asked for certain information, which it is not up to this Authority to provide.

Without prejudice to the above, the information requested by the reporting person could come to highlight a possible breach of article 32 of the RGPD (relating to data security), which in his case could become constitutive of the infringement provided for in article 83.4.a) of the RGPD, which typifies as an infringement the violation of the obligations of the person in charge provided for in various precepts of the RGPD, among which article 32 of the RGPD. For its part, article 73 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), has included as a serious infringement both the lack of adoption of the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk of the treatment (art. 73.f), such as non-compliance with the security measures implemented (art. 73.g).

Likewise, article 73 of the LOPDGDD also provides that serious infractions have a two-year statute of limitations. Considering that the audit was requested on 12/12/2018, the eventual breach of data security would have prescribed (on 12/11/2020), i.e. a few days after submitting - the complaint (11/13/2020).

The prescription of the infringement causes the extinction of the responsibility that could be derived from the eventual infringing conduct, which in turn would prevent the initiation of the corresponding sanctioning procedure, since no action could be taken to pursue the alleged infringement .

On the other hand, the complainant also requested to know the reason why the rest of the 12,500 audited SIP consultations were dismissed (that is, not imputed within the framework of the disciplinary proceedings instituted by the City Council against the complainant and another agent).

Nor is it up to this Authority to resolve this query of the reporting person. In any case, it is logical to infer that if certain audited SIP consultations were not included among the facts attributed to the two GU agents to whom it was

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

initiate a disciplinary file, this would probably be motivated by the fact that the City Council would have no evidence to consider that those consultations were illegal.

3. In accordance with everything that has been set out in the 2nd legal basis, and given that during the actions carried out in the framework of the previous information it has not been accredited, in relation to the facts that have been addressed in this resolution, no fact that could be constitutive of any of the violations provided for in the legislation on data protection, should be archived.

Article 89 of the LPAC, in accordance with articles 10.2 and 20.1 of Decree 278/1993, foresees that the actions should be archived when the following is highlighted in the instruction of the procedure: "c) When the proven facts do not manifestly constitute an administrative infraction".

Therefore, I resolve:

1. File the actions of prior information number IP 342/2020, relating to the City Council of (...).

2. Notify this resolution to the City Council of (...) and to the person making the complaint.

3. Order the publication of the resolution 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 article 14.3 of Decree 48/2003, of 20 February, which approves the Statute of the Catalan Data Protection Agency, the persons interested parties may file, as an option, an appeal for reinstatement before the director of the Catalan Data Protection Authority, within one month from the day after their notification, in accordance with what provided for in article 123 et seq. of Law 39/2015. An administrative contentious appeal can also be filed directly 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, governing the contentious administrative jurisdiction.

Likewise, interested parties may file any other appeal they deem appropriate to defend their interests.

The director,