

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 274/2020, referring to the City Council of (...).

#### Background

1. On 09/14/2020, the Catalan Data Protection Authority received a letter from a person who lodged a complaint against the City Council of (...), on the grounds of an alleged non-compliance with the regulations on personal data protection.

Specifically, the complainant (an officer of the Local Police of (...)) stated that on 09/20/2019, by email, the head of the Local Police of (...) went alone request the Division of Police Information Systems (DSIP) of the Directorate General of Police (DGP) of the Department of the Interior to conduct an audit on the Police Information System (SIP) queries made to certain municipally owned vehicles by the users of the Local Police of (...).

The complainant stated that in said e-mail, the head of the Local Police informed the DSIP that he had "decided to make confidential information in order to initiate a disciplinary procedure". However, the complainant

pointed out that it was not until 17/10/2019, when the mayoress of the City Council of (...) decided to initiate a file of reserved information in order to verify the facts reported by the accidental chief sergeant of the Local Police in its report dated 04/10/2019. For this reason, the complainant considered that the aforementioned audit was requested before the information file was initiated by the competent body (the mayoress), so this treatment would be illegal.

The reporting person provided various documentation relating to the events reported.

2. The Authority opened a preliminary information phase (no. IP 274/2020), 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 this information phase, on 21/09/2020 the reported entity was required to report, among others, on the reasons why in the mail of 20/09/2019 information was given about the decision to open confidential information, which was not agreed upon

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

start until 10/17/2019; as well as on the specific legal basis that legitimized the request for an audit to the DSIP on the accesses to the SIP made to consult certain vehicles owned by the municipality.

4. On 10/05/2020, the City Council of (...) responded to the aforementioned request through a letter in which it stated the following:

- That the head of the Local Police had evidence that, allegedly, some agents would have used the SIP of the DGP for purposes other than those of the Local Police service.
- That the head of the Local Police requested, on 09/20/2019, a specific audit of the data consulted by the Local Police officers, specifically of municipally owned vehicles, in order to know if it could be to have committed any alleged offense subject to the disciplinary regime and request, in such case, the opening of reserved information.
- That this audit was available on 09/30/2019.
- That the head of the Local Police verified that two Local Police officers and a corporal had accessed the SIP for purposes other than those of the municipality's police service, which prompted the issuance of a report addressed to Mayor's office on 04/10/2019, requesting the opening of a reserved information file in order to investigate the facts and determine whether they constituted a disciplinary file.
- That this file was started on 10/17/2019.
- That in carrying out a mission carried out in the public interest or in the exercise of public powers, in accordance with article 6.1.e) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 of April, relating to the protection of natural persons with regard to the processing of personal data and the free circulation thereof (hereinafter, the RGPD), the head of the Local Police, as responsible for the police force, receives on a monthly basis an audit of the inquiries made by the agents of the staff in a generic form and it is this same legal basis that legitimizes him to request a specific audit to consult the accesses to the SIP made to consult certain ownership vehicles municipal
- That Law 16/1991, of July 10, on the local police (hereinafter, Law 16/1991) states in its article 27.a) that it is up to the head of the body to ensure the operational and administrative supervision of the body of the Local Police.
- That article 24 of Law 4/2003, of April 7, on the organization of the public security system of Catalonia, regulates the possibility that the local police forces, through an agreement, can participate in the unified system of police information, use the computer software applied to the police of the Generalitat-mossos d'esquadra and work in integrated networks of police information.
- That the security audit of the system is regulated in clause 11 of the agreement on the connections to the police information system between the Department of the Interior and the City Council of (...), in which it is foreseen that the Department of the Interior, as holder of the

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

SIP may, at any time, inspect the facilities, security mechanisms and personnel responsible for accessing the system.

- That among the functions of the head of the Local Police of (...), is that of directing and supervising the activities of the staff in his charge. The head of the Local Police is also the computer interlocutor in the local area of SIP management, in accordance with what is established in clause 7 of the agreement on connections to the police information system. It is also established in this same clause of the agreement that the IT contact person at the local level (the head of the Local Police) must ensure the security of the system in accordance with the criteria established by the security manager of the SIP and must perform the functions that are included in the safety manual. Especially, it must guarantee that the other users of the Local Police make correct use of it.
- In use of these functions and in order to control that the staff of the Local Police use the SIP in accordance with the provisions of the agreement that regulates the connections to the local information system, the head of the Local Police shall request an audit of the data consulted by the Local Police officers, specifically of municipally owned vehicles.

The reported entity attached various documentation to the letter.

#### 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 account of facts that has been set out in the background section, it is necessary to analyze the reported facts that are the subject of this file resolution.

In the present case, it is reported that the head of the Local Police of (...) asked the DSIP for an audit on access to the SIP by the Local Police officers, without having initiated a reserved information.

As indicated in the report issued by the head of the Local Police on 04/10/2019 (provided by the person reporting), on 21/08/2019 he became aware that the person reporting here, as a union delegate, presented an instance to the City Council regarding several irregularities regarding the ITV and the insurance of the vehicles, in service or not, attached to the Local Police of (...). In the same report it was also highlighted that, on (...), La Vanguardia published a news related to a trade union complaint about the condition of the vehicles attached to the Local Police, where it was mentioned that the trade union representatives they had admitted the precarious situation with which they worked.

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

Given the above, the head of the Local Police of (...) requested on 20/09/2019 to the DSIP an audit "between 1/8/2019 and 21/08/2019 regarding the inquiries made of vehicles owned by the municipality" which he detailed, through the SIP.

In accordance with article 27 of Law 16/1991, it corresponds to the head of the Police Venue:

- "a) Direct, coordinate and supervise the operations of the body, and also the administrative activities, to ensure their effectiveness.
- b) Assess the needs of human and material resources and formulate the relevant proposals.
- c) Transform into concrete orders the guidelines for the objectives to be achieved, received from the mayor or the office to which he delegates.
- d) Inform the mayor, or the position to which he delegates, of the operation of the service.
- e) Fulfill any other function attributed to him by the body's municipal regulations."

As stated by this Authority in the archive resolution of the previous information number IP 52/2020, in the exercise of these functions, the head of the Local Police may request an audit of access to the SIP. In fact, in the agreement on the connections to the Police Information Systems signed between the Department of the Interior and the City Council of (...) it is specified that the IT interlocutor in the local area of SIP management is the head of the Local Police or another police officer designated by him (in the present case, the City Council specified that the IT interlocutor was the own head of the Local Police). As specified in the said agreement, the IT contact person at the local level must ensure the security of the system in accordance with the criteria established by the SIP security manager and must perform the functions that are included in the safety manual. In particular, it must ensure that the other users of the Local Police use it correctly. To this end, the aforementioned interlocutor must notify the head of the Information Technology Security Area of the DGP immediately of any incident, that is, any anomaly that affects or may affect the security of SIP data, in accordance with what is established in the security manual.

As things stand, the head of the Local Police is the person authorized to request an audit of SIP access to the Department of the Interior. Even if he had not been designated as an IT interlocutor, he would still be authorized to request an audit on access to the SIP taking into account the functions attributed to him by Law 16/1991.

As stated before, in the present case there were indications (an instance presented by the person making the complaint before the City Council and the news published in the media) that allowed us to infer that the SIP would have been accessed to consult information

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

linked to the vehicles attached to the Local Police, without this being justified, in appearance, in the exercise of their duties entrusted to the officers of the Local Police.

At this point, 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 users who access it.

Article 5.1.f) of the 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 or illegal processing lawful and against the loss, destruction or accidental damage of the data, through the 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 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 Local Police was based on 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 RGPD and Law 16/1991. In turn, the performance of the audit by the DGP would also be based on the legal basis provided for in article 6.1.e), as well as the fulfillment of a legal obligation (art. 6.1.c RGPD) which derives from the RGPD (arts. 5.1.f) 32).

On the other hand, the complainant stated that in the e-mail of 09/20/2019 through which the head of the Local Police requested the DGP to audit access to the SIP, it was pointed out that "decided to make confidential information in order to initiate a disciplinary procedure", although it is proven that until 17/10/2019, the mayor of the City Council of (...) did not decide to initiate a reserved information file.

In this regard, it should be emphasized that the adoption of security measures, such as an audit of accesses aimed at guaranteeing the security of data in

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

compliance with article 32 of the RGPD, is not subject to the fact that the competent body can open a period of information or prior actions in order to know the circumstances of the specific case and the convenience or not of starting the procedure, and this because data security must be guaranteed at all times.

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.

Therefore, I resolve:

1. File the actions of prior information number IP 274/2020, 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,