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 73/2021, referring to the City Council of (...).

Background

1. On 18/02/2021, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the City Council of (...), on the grounds of an alleged non-compliance with the regulations on the protection of personal data, and in the same letter also denounced a complaint against a certain action of
the Basic Police Area of (...) (hereinafter, ABP) in response to a request from a Court.

Specifically, and with regard to the City Council of (...), the complainant stated the following:

1.1. That on (...) the chief inspector of the Urban Guard of (...) sent an email to the head of the Information Technology Security Area of the Police Information Systems Division (henceforth, DSIP) of the Directorate General of Police (DGP) of the Department of the Interior, through which he requested that the complainant be deregistered as a SIP user. As grounds for complaint, the complainant stated, on the one hand, that this email had not been sent

sent in encrypted form, as established in the SIP Security Manual; and on the other hand, that the mail had been sent to the head of the DSIP, when the aforementioned Security Manual indicates that these user cancellation request mails should not be sent to said head.

1.2. The reporting person stated, in an imprecise manner, that audits had been requested "without objective data" from a person who was not responsible, referring to the head of the ABP of (...). The reporting person did not provide any documents to substantiate these reported facts.

1.3. Finally, he requested access to various information.

The complainant provided a copy of an official document issued on 07/08/2020 by the head of the aforementioned ABP, addressed to the said Court of First Instance and Instruction (...) of (...), in which stated the following:

> "In response to his office (...) we inform you that, according to the Audit Unit of the Police Information Systems Division states that:

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

> On date (...), the chief inspector of the Urban Guard of (...), Mr. (...) -name and surname requested, via email addressed to the head of the Information Technology Security Area of the Police Information Systems Division, that it be blocked urgently immediately access to the user's SIP (...)
> - first and last name of the person making the complaint - since a disciplinary file had been opened against him by mayoral decree no. (...), dated (...)."

2. In relation to the reported events relating to the actions of the City Council of (...) the Authority opened the current preliminary information phase (no. IP 73/2021), in accordance with what provides for article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, of the common administrative procedure of public administrations (henceforth, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

With regard to the facts reported relating to the performance of an ABP of the Police of the Generalitat Mossos d'Esquadra, assigned to the DGP of the Department of the Interior, the Authority opened the preliminary information phase no. IP 73bis/2021.

In this resolution, the reasons for the complaint referred to the actions of the City Council of (...) described in the background are addressed.

3. On 26/02/2021, the Authority required the reported entity to specify whether the controversial email from the chief inspector of the Urban Guard (GU) of (...) (background 1, section 1.1 .), had been sent in encrypted form.

4. On 03/15/2021, the City Council of (...) responded to the aforementioned request through a letter in which it stated the following:

> "The City Council of (...), works on the application and compliance of sufficient and necessary security measures in accordance with the applicable regulations and detected risks.
>
> That in the context of this previous information, the email that was sent to the head of the Security Area in Information Technologies was in relation to a request to deregister a user of the Local Police SIP application .
>
> That the Manual of additions, deletions and modifications of users of the local police to the SIP of the DGP establishes: Any request sent by an unauthorized, incorrectly filled or unencrypted mailbox will be denied.
>
> That the City Council of (...) is not aware of, nor has it been able to verify, whether the email in question was sent encrypted because access to emails from

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

workers with the exception of exceptional cases in the context of suspected violations of protocols and regulations."

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 encryption of the email through which SIP user cancellation was requested, and about the person to whom said email was sent.

First of all, the complainant stated that on (...) the chief inspector of the Urban Guard of (...) sent an unencrypted email to the head of the DSIP, in order to give him log off as a SIP user, contravening the provisions of the SIP Security Manual (precedence 1).

The aforementioned Security Manual is incorporated as annex 2 to the agreement on the connections to the Police Information Systems signed between the DGP and the City Council of (...) (which was provided together with the complaint that gave rise to sanctioning procedure no. PS 45/2019). Section 2.2 of this Manual refers to the communications made between the IT interlocutor in the area of the Local Police connected to the SIP and the security manager of the SIPs, and it is certainly clear from its reading that it is mandatory to encrypt or encrypt e-mail messages containing SIP user unsubscribe requests, as follows:

> "(...) The transmission of confidential information via e-mail such as user codes and pass keys to access the SIPs, the names and surnames of the holders of the codes, as well as other types of 'information related to these systems will have to be made mandatory through the encryption of email messages and their attached documents.

On the other hand, in the same section of the Safety Manual, the following address is indicated email address of the DGP user service (Help Desk) to which, among others, requests to unsubscribe from users should be sent:

- (...): intended for user registration and cancellation communications, incidents, inquiries, etc.

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

and then the following is indicated:

> "messages will be sent to one of these addresses - including the one indicated above - as the case may be, and sending to the direct addresses of those responsible for the DSIP will be avoided for the cases described here."

Based on this content of the Security Manual, the reporting person considers that the head of the GU of (...) contravened this Security Manual by having sent the e-mail to the head of the DSIP (instead of 'send it to the email address indicated in the Manual), as well as for having sent it unencrypted. With this complaint, the complainant refers to the possible violation of the duty of confidentiality and a measure
of security.

In this sense, article 5.f) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free circulation of these (RGPD), provides that personal data must be treated in such a way as to guarantee adequate security, through the application of appropriate technical or organizational measures. Next, the two grounds of complaint referred to the sending of this will be analyzed separately
mail

2.1.1. First of all, regarding the sending of the email to the head of the DSIP, which the City Council has confirmed, it must be noted at the outset that from the reading of section 2.2. of the SIP Security Manual ("...sending to the direct addresses of those in charge will be avoided"), it is not clear that this type of mail cannot be sent to the head of the DSIP, in the sense of the rule of prohibition, but that this provision could obey operational reasons or the organization of the service, in the sense of considering that the sending of requests for additions and deletions of SIP users to specific addresses, allows to manage better these requests. In the interpretation of this section 2.2 of the Security Manual, the fact is taken into account that the head of the DSIP to whom the mail was sent, is the most responsible of the unit in charge of managing the police information system (Decree 415/2011, of 13 December, on the structure of the police function of the Directorate General of Police). So I could access the
requests to deregister SIP users in practice or for the fulfillment of assigned functions.

On the other hand, it must be noted that clause 5.7 of the aforementioned agreement signed between the DGP and the City Council of (...), could prevent the mail from being sent to the head of the DSIP. This clause 5.7 is entitled "computer interlocutor in the local area and users", and indicates that the interlocutor "must be the Chief of the Local Police or another local police officer designated by him", and that this interlocutor "has to send to the head of the Security Area in

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

Information Technologies" certain information, which includes, for what is of interest here, the following:

- "Immediately communicate all changes to users, must request user registrations and cancellations when a user ceases to belong or provide services, for any reason, to the Local Police.

- Communicate immediately any incident, that is, any anomaly that affects or may affect the security of the SIP data, in accordance with what is established in the Security Manual."

The present case could be relevant to the cases transcribed, since the request to deregister the user was due to the fact that the City Council had instituted disciplinary proceedings against him for alleged illicit access to the SIP, and an injunction had been adopted. In other words, with the mail sent by the chief inspector of the GU of (...)
to the head of the DSIP, he communicated the incident that affected the security of the SIP data, and linked to this, he urgently formulated the request for termination as
SIP user to the person who allegedly illegally accessed the SIP. In such a case, the sending of the mail by the head of the GU to the head of the DSIP, would be based on the fulfillment of a legal obligation in accordance with articles 6.1.c) and 5.1.f) 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.

According to the reasons indicated, it is not observed with the necessary clarity that the fact of having sent an email to the head of the DSIP, constitutes an infringement. But even if that were the case, it is considered that these facts do not have sufficient substance to initiate disciplinary proceedings, given the circumstances indicated.

2.1.2. Secondly, regarding the sending of the unencrypted email, the City Council of (...) has stated, by means of a letter dated 03/15/2021, that "it is not aware of nor has it been able to verify whether the The email in question was sent encrypted." And in his answer he also referred to the point in the Security Manual where it is pointed out that: "any request sent by an unauthorized, incorrectly filled or unencrypted mailbox will be denied", implying that if the City Council had had the mail been sent unencrypted, the user deregistration request would have been denied, which did not happen, as the DSIP deregistered the complainant from the SIP.

Thus things, the statements made by the person making the complaint, without providing any evidentiary element to substantiate them -even if it is circumstantial-, seem to be mere suspicions, which by themselves do not allow to infer that the City Council could have committed the offense pointed out, and consequently start a sanctioning procedure.

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

But even if that were the case, it would not be appropriate to start the challenge action due to the fact that the possible infringement committed would be time-barred, taking into account that the email in question was sent on 03/04/2019.

Indeed, article 83.4.a) of the RGPD typifies as an infringement the violation of the obligations of the person in charge provided for in several precepts of the RGPD, among which is the encryption of personal data (art. 32.1.a 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 infraction the breach of the security measures implemented (art. 73.g).

Article 73 of the LOPDGDD provides that serious infringements have a two-year statute of limitations. Well, at the time the present resolution was issued, this limitation period would have passed. In this assessment of the calculation of the deadline, the period of suspension of the deadline provided for in additional provision 4a of Royal Decree 463/2020 of March 14, by which the state of alarm will be declared for the management of the health crisis situation caused by the COVID-19. Consequently, in the unlikely event that it is considered that the facts reported constitute an infringement, this would have prescribed, which causes the extinction of the responsibility for the eventual infringing conduct.

2.2. On requests for audits made without legal cause and addressed to an incompetent person.

Next, the reporting person stated, in an imprecise manner, that audits had been requested "without objective data" from a person who was not responsible, and referring to the head of the ABP of (...) , as follows: "that the request for audits...do not comply with the law in that without objective data an audit is requested from someone who is not responsible (Head of the ABP of (...) ) to try to find a fact that leads to requesting another audit (...)".

The truth, however, is that the complainant did not specify which audits he was referring to, nor did he provide any documents to substantiate the facts he was reporting, nor did he mention the rule that in his opinion would have been contravened.

Despite this inaccuracy, everything seems to indicate that the complainant could be referring to an audit request made by the head of the GU of (...) on 12/12/2018.

With respect to this audit request, the complainant already filed a previous complaint with the Authority (which led to the opening of IP 342/20), through which he stated that this request of audit was illegal, since neither the real reason for requesting it, nor the purpose pursued, was in accordance with the law. In that case, after the appropriate investigative actions, the Authority issued a filing resolution, dated

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

10/18/2021, to consider that both the audit request and its performance were legitimate, as follows (foundation of law 2.1:

> "(...) 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 draw up an audit corresponds is the data controller, that is to say, 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 that the purpose pursued is to guarantee the security of the data included in said information system."

That being the case, with regard to these reported facts, it must be concluded that the reporting person has not provided elements that substantiate the facts he reports, nor, consequently, elements from which it can be inferred that the City Council of (...) could have committed an offence. And in any case, regarding the audit request that the head of the GU of (...) formulated on 12/12/2018, and in the audit itself, the Authority already pronounced on the legitimacy of the aforementioned data treatments.

2.3. On other issues raised by the complainant.

In the last one, the complainant requested to know certain information, as follows: "I request to know from which e-mail the request was made and to which e-mail it was made, in order to confirm whether comply with the law and the aforementioned protocol (...) That I be clearly informed of the times that my queries have been audited in the SIP application, as well as knowing the reasons that led to it".
In this regard, it is sufficient to point out that with these manifestations, the reporting person is not reporting any conduct contrary to the regulations on data protection, but is asking for certain information, which it is not up to this Authority to provide.

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

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, or in any case these would have prescribed, should be archived.

Article 89 of the LPAC, in line 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 "a) The non-existence of facts that could constitute the infringement; b) When the facts are not proven; c) When the proven facts do not manifestly constitute an administrative infraction"; e) When it is concluded, at any time, that the infringement has prescribed".

Therefore, I resolve:

1. File the actions of prior information number IP 73/2021, 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,