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 52/2021, referring to the City Council of (...).

Background

1. On 03/11/2020, the Catalan Data Protection Authority received two letters from the same person in which he filed a complaint against the City Council of (...), on the grounds of a alleged breach of the regulations on personal data protection.

Specifically, the complainant stated, among others, the following:

1.1. That in the report issued on 01/02/2019 by the chief inspector of the Urban Guard of (...) -henceforth, GU- (by which the report issued on 27/12/2018 was expanded in which it was requested to initiate investigative proceedings against two officials of the GU for allegedly improper access to the Information System Police - henceforth, SIP-) contained the personal data that another GU agent had consulted through the SIP.

1.2. That while he was on leave, the Chief Inspector of the GU acceded to an instance that was presented (at the end of January 2019) by the representative of a certain political party (Mr. (...)), as it is confirmed in the report of 02/01/2019. He adds that the disciplinary file initiated by the City Council is based on several reports drawn up by the chief inspector of the GU also drawn up when he was on leave.

1.3. That the union representatives were informed, the initiation of the proceedings disciplinary measures imposed on the reporting person and another agent.

1.4. That the Candidature of Popular Unity (hereinafter, CUP) was informed about the initiation of disciplinary proceedings (initiated by the City Council against the complainant and another agent of the GU); as well as to the people affected by the consultations in the SIP that motivated the initiation of a disciplinary file (to the reporting person and to another officer).

1.5. That in the report issued by the chief inspector of the GU on 26/06/2019 (in relation to the possible dilatory practice of the people filed in order for the disciplinary procedures to expire), it contains information regarding the other agent of the GU against whom a disciplinary file was also initiated.

1.6. That as can be seen from the report of 01/02/2019 mentioned above, 12,500 inquiries made through the SIP were verified (6,500 in relation to physical persons and 6,000 in relation to vehicles), but that in the framework of only a small part of them were included in the disciplinary record. The complainant also questioned

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

how the information related to inquiries that would not have been considered illicit was guarded.

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

The number IP 333/2020 was assigned to this complaint.

2. The Authority opened a preliminary information phase, in accordance with the provisions of 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 (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

3. On 14/11/2020, the complainant submitted a new letter of complaint against the City Council of (...) in which he stated the following:

3.1. That the City Council of (...) manipulated 12,500 files (consultations) of the SIP (which would have been carried out by the complainant and another agent), without the minimum security requirements.
3.2. That the initiation of disciplinary proceedings have been communicated to political parties (the CUP) and to the people affected (a fact I had already denounced, as stated in background 1.4), such as Mr. (...).

The complainant provided various documentation.

This complaint was assigned IP number 344/2020.

4. In this information phase, on 09/12/2020 the reported entity was required to report, among others, on the reasons why the reporting person was provided with the report of 01/02 /2019, without anonymizing the data relating to another agent, nor the data relating to third parties linked to the SIP accesses that this other agent made; if the chief inspector of the GU was on sick leave when he acceded to the instance that had been presented by Mr. (...) in front of the City Council; if the people to whom the head of the Personnel and Organization Department communicated, by email, the initiation of two disciplinary proceedings were staff delegates or members of the staff board; the reasons why the reporting person was provided with the report of 06/26/2019, without anonymizing the information regarding the other GU agent against whom disciplinary proceedings were also initiated; and in relation to the 12,500 consultations in the SIP, carried out by the expedient agents, to which the report of 02/01/2019 refers, it was required to provide a copy of the risk analysis used to determine the measures to guarantee the security of this data in the City Council's systems.

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

5. On 31/12/2020, the City Council of (...) responded to the aforementioned request through a letter in which it set out, among others, the following

- That the report of 01/02/2019 without anonymization, was provided by the then head of Personnel, who no longer works at City Hall
- That it is unknown when the head of the GU acceded to the instance presented by Mr. (...). The head of the GU was on leave from 13/12/2018 to 15/02/2019.
- That the legal basis for access to said instance derives from article 27 of the Law 16/1991, of July 10, of the local police (hereinafter, Law 16/1991).
- That in relation to the e-mail through which the initiation of two files would have been communicated, the current head of personnel in office does not have access to the e-mail (the head of personnel who sent the e-mail no longer works at the Town hall). It was only possible to access the screenshot provided by the APDCAT [which had been provided by the reporting person and where only 2 of the 5 recipients were identified], so it was only possible to know the details of two people, (...) and (...), which were members of the Personnel Board.
- That the report of 06/26/2019, without anonymization, was provided by the then head of Personnel who no longer works at City Hall.
- That the only person who could request an audit of SIP access was the Head of the GU, which at the time of responding to the request was on leave.
- That the City Council's personnel and organization team and its acting heads do not have this audit, the Head of the GU should be asked. Nor do they have the risk analysis that may have been carried out.
- That the persons authorized to access this documentation (the audit of SIP access) are the head of the GU, the councilor and the mayor.
- That in relation to the SIP consultations, carried out by the expedient agents, is don't know if they were deleted or blocked.

6. On 01/15/2021, the complainant submitted a new letter of complaint, in which he stated the following:

6.1. That the head of the GU requested an audit from the Department of the Interior, despite not being the IT interlocutor, contravening the Security Manual of the connection agreement of the local police to the SIP.

6.2. That said request, which would include, according to the complainant, "the user codes and Passkeys to access the SIPs, the names and surnames of the holders of the codes", was made by unencrypted email (the said manual provides that the communication of user codes, the pass keys to access the SIP and the names and surnames of the holders of the codes, must be done by means of encryption of e-mail messages and their attachments).

The reporting person provided a copy of the Security Manual of the connection agreement of the local police to the SIP of the DGP. In this manual, it is specified that the "sending of confidential information [to the DGP] 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 must be done by encrypting email messages and their attached documents."

This complaint was assigned IP number 18/2021.

7. On 03/03/2021, the City Council of (...) was again requested so that, in the event that the head of the GU was not on leave, he would report on certain aspects. And, in the case that he was still on leave, and in relation to the 12,500 consultations in the SIP, carried out by the agents in charge, the testimony of the councilor or the mayor was required as to whether they could access said documentation (the 12,500 consultations in the YUP); whether a risk analysis had been carried out to determine the measures to guarantee the security of this data in the City Council's systems; as well as if the information linked to the consultations that were not considered illegal (that is, those that were not the subject of disciplinary proceedings), had been deleted or blocked.

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

- That the chief inspector of the GU was still on leave.
- That the mayor and the councilor at the time of the report issued on 01/02/2019, are no longer part of the Consistory.
- 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 recorded that any data had been deleted or blocked from any municipal or supra-municipal register in relation to the consultations carried out.

9. On 07/26/2021, the person making the complaint submitted a new letter in which he indicated that the City Council of (...) would have provided a list of people affected by improper access to the SIP (made by the person here making the complaint and another agent) to Mr. (...) (person whose data was consulted in the SIP).

The complainant provided various documentation.

In accordance with the antecedents that have been related so far and with the result of the investigative actions carried out in the framework of the previous information, it is agreed to initiate this sanctioning procedure. In the following sections, all the information required by article 64.2 of the LPAC is indicated.

10. On 18/10/2021, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the City Council of (...) for an infringement provided for in article 83.4.a) in in relation to articles 5.1.f), 32.1 and 2, all of them of the Regulation

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

(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 movement thereof (hereafter, RGPD). This initiation agreement was notified to the imputed entity on 10/20/2021.

11. In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of tests that it considered convenient for defend their interests. The deadline has been exceeded and no objections have been submitted.

12. The initiation agreement explained the reasons why no imputation was made with respect to other facts reported.

12.1. Regarding the delivery of reports (background 1.1 and 1.5), the resolution of the Director of the Authority of 01/21/2021, in procedure no. PS 47/2020, sanctioned the City Council of (...) for facts that together with this fact constituted a plurality of actions in execution of a preconceived plan or taking advantage of an identical occasion. These actions
they infringe the same precept (art. 83.5.a of the RPGD, which typifies as an infringement the violation of the principle of legality contemplated in articles 5.1.ai and 6 of the RGPD). It is about of a continued infringement that was already sanctioned by this Authority. Therefore, the "non bis in idem" principle that is included in article 31.1 of the LRJSP applies here.

12. 2. On the situation of leave of absence of the head of the GU (background 1.2). Both the reports issued by the head of the GU and the access to the referred instance are treatments that would have been carried out in the exercise of the functions of supervising the body's operations and administrative activities, which article 27.1 of Law 16/ 1991 attributed to the head of the GU. The above, together with the seriousness of the facts (which the head of the GU considered could constitute a criminal offense) would justify that, despite being on leave, the head of the GU issued said reports for certain facts linked to the SIP.

12.3. On the communication of the initiation of disciplinary proceedings to the people affected by access to the SIP and the CUP (background information 1.4, 3.2 and 9). The resolution of the director of the APDCAT of 01/21/2021, which put an end to sanctioning procedure no. PS 47/2020, sanctioned the City Council of (...) for these same facts, which is why the "non bis in idem" principle also applies here. And as for an eventual
list of people affected by illicit access to the SIP, there is no minimally indicative element that allows us to infer that the City Council had disseminated the aforementioned list. This reported fact is based on a mere assumption.

12.4. On the communication of the initiation of disciplinary proceedings to union representatives (precedent 1.3). The communication to the Personnel Board of the agreement to initiate the disciplinary file against the person reporting here, in the

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

terms that was carried out, it was enabled by a standard with the rank of law (DL 1/1997), which carries out a regulatory referral. Therefore, this treatment is lawful in accordance with article 6.1.c) of the RGPD.

12.5. On the request for the SIP access audit (background 1.6 and 6.1). As reported by the DGP in the framework of the previous information no. IP 334/2020, it is not up to the IT interlocutor (who would be the person reporting here at the time the audit was requested) to request audits on access to the SIP, but that audit requests have to carry out the Chiefs of Local Police. In addition, 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 audit by the DGP would also be based on the same legal bases.

12.6. On the encryption of the mail through which the SIP access audit was requested (background 6.2). The complainant did not provide a copy of said email, so it has not been possible to check whether it was actually sent and what its content was (whether it included passwords, names and surnames, etc.). Nor was there any slightest indication that would allow us to infer that, in the event that the mail had included the controversial data, this security measure, which is determined in the Security Manual of the connection agreement of the local police forces, had not been implemented YUP. But, even in the unproven case that the eventual infringement linked to the sending of said unencrypted e-mail had occurred, this infringement was already time-barred when these facts were reported on 01/15/ 2021 The prescription of the infringement causes the extinction of the responsibility that could be derived from the eventual infringing conduct.

proven facts

The City Council of (...) did not certify that it had carried out a risk analysis to determine the appropriate technical and organizational measures to guarantee the security of personal data that are processed within the framework of disciplinary procedures, such as those linked to 12,500 inquiries to the SIP made by the complainant and another agent (all inquiries made by them between 08/01/2017 and December 2018) which were the subject of an audit (for the purpose of the City Council investigating whether they were carried out by said agents in the exercise of their functions or not) and to which the report issued by the head of the GU on 01/02/2019 refers.

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 Authority

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

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. In accordance with article 64.2.f) of the LPAC and in accordance with what is indicated in the agreement initiating this procedure, this resolution should be issued without a previous resolution proposal, given that the accused entity has not made allegations in the initiation agreement. This agreement contained a precise statement of the imputed liability.

2. In relation to the facts described in the proven facts section, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data (hereafter, RGPD), article 5.1. f) of the RGPD that regulates the principle of integrity and confidentiality determines that personal data will be "treated in such a way as to guarantee adequate security of personal data, including protection against unauthorized or illegal treatment and against loss, destruction or accidental damage, through the application of appropriate technical or organizational measures".

For its part, article 32.1 of the RGPD, which provides that "Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of variable probability and seriousness for the rights and freedoms of physical persons, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk (...)."

In turn, article 32.2 of the RGPD provides that "When evaluating the adequacy of the security level, particular consideration will be given to the risks presented by data processing, in particular as a consequence of accidental destruction, loss or alteration or illegal transfer of personal data, stored or otherwise processed, or unauthorized communication or access to said data." This implies having to carry out an assessment of the risks involved in each treatment, in order to determine the security measures that need to be implemented.

During the processing of this procedure, the fact described in the proven facts section, which is constitutive of the violation provided for in article 83.4.a) of the RGPD, which typifies as such the violation of "the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43", among which there is that provided for in article 32 RGPD.

The conduct addressed here has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

> "f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679."

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

3. 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 conduct ceases or the effects of the offense committed are corrected.
>
> The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to 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 violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".

By virtue of this power, it is necessary to require the City Council of (...) so that as soon as possible, and in any case within the maximum period of 20 days from the day after the notification of this resolution, carry out a risk analysis to determine the appropriate technical and organizational measures to ensure the security of personal data that are processed within the framework of disciplinary procedures.

Once the corrective measure described has been adopted within the period indicated, within the next 10 days the City Council must inform the Authority, without prejudice to the Authority's inspection powers to carry out the corresponding checks.

For all this, I resolve:

1. Admonish the City Council of (...) as responsible for an infringement provided for in article 83.4.a) in relation to articles 5.1.f) and 32, all of them of the RGPD.

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

2. Request the City Council of (...) to adopt the corrective measure indicated in the 3rd legal basis and accredit before this Authority the actions carried out by
fulfill it

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

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

5. 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 what they provide
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,