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 31/2021, referring to the City Council of (...).

Background

1. En data 19/02/2020 va tenir entrada a l'Autoritat Catalana de Protecció de Dades, per remissió de la l'Agència Espanyola de Protecció de Dades (en endavant, AEPD), un escrit d'una persona pel qual formulava complaint against the City Council of (...), due to an alleged breach of the regulations on the protection of personal data.

Specifically, the complainant (local police officer from (...)) stated that, on 16/12/2019, the City Council had decided to remove his firearm (file (...)) ). He added that this file and the one that had been assigned to another colleague (file (...)) could be consulted through the municipal intranet by all users who had access to it. The complainant stated that he became aware of this circumstance, once he found out on 12/17/2019 that "different citizens of the municipality" had evidence that he was in a situation of unemployment, which had led to his being withdrawn firearms - service and personal - to be a medical leave due to mental deficiencies. The complainant provided various documentation.

2. The Authority opened a preliminary information phase (no. IP 71/2020), 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 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 04/06/2020 the reported entity was required to inform, among others, about the people who could access the information system where the previously identified files were stored concerning two officers of the Local Police; as well as if, prior to 16/12/2019, a risk analysis had been drawn up regarding the documentation stored in said information system.

4. On 16/06/2020, the City Council of (...) responded to the aforementioned request through a letter in which it set out, among others, the following:

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

- That the files (...) and (...), in electronic form, were not stored on the intranet, but in the file manager.
- That these files were from the Citizen Security Area. Citizen Security files could only be accessed by people assigned as members of the Citizen Security Area in the file manager (file manager user category).

- That to facilitate access to the file manager there is a link on the intranet, but the link does not imply free access to the file manager, but only for the people assigned to the Citizen Security Area in the file manager. Identification is done by means of a user code and password or a digital certificate.
- That the City Council of (...) and the Regional Council of Vallès Oriental have an information and communication technology collaboration agreement for the year 2017. In this agreement, they are established as obligations of the Regional Council to transfer the use of the file manager to the City Council, to take care of the maintenance of the file manager, to manage and supervise the deployment project of the file manager and to manage the configuration and parameterization of the system .
- That prior to 01/22/2020, users (32 in total) who were assigned to the Citizen Security Area could access the files. Other users of the file manager could not access it.

- That on 22/01/2020, at the request of the City Council, the Information and Communication Technologies Service of the Regional Council of Vallès Oriental modified the category of users corresponding to the Citizen Security unit in the manager of files, allowing access only to authorized users (the City Council identified the 7 people from the Citizen Security Area who continued to be part of the "Citizen Security Unit" user category of the file manager) .
- That, prior to 12/16/2019 (date on which the City Council decided to remove the firearm from the person making the complaint), the City Council had not prepared a risk analysis in relation to the documentation stored in the file manager.

The reported entity attached the report of the Information and Communication Technologies Service of the Regional Council of Vallès Oriental, issued on 06/12/2020. This report stated, among others, the following:

- That, following the directions of the City Council, 32 users were assigned to the Citizen Security unit (who were identified and among whom was the complainant). These 32 users, on 16/12/2019, could have access to the files (...) and (...), in electronic support through the file manager.
- That, on 22/01/2020, the Security unit was modified at the request of the City Council Citizen, this category of users being integrated by 7 people.

In said report, the record of the inquiries made to the controversial files ((...) and (...)) between 12/12/2019 and 06/08/2020 through the file manager was incorporated .
This record showed that, until 12/17/2019 (the date on which the reporting person

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

stated that he had been aware that several citizens of the municipality had records of his absence from work and of the withdrawal of weapons) only a single user had accessed the files ("(...)"). At the time of making the inquiries, this person was part of the "Citizen Security Unit" users of the file manager (user category included at the time of the inquiries by 32 people). As of 22/01/2020 (the date when said category of users was reduced to 7 people) this user person continued to be part of the category of users of the file manager called "Citizen Security Unit" .

5. On 06/25/2020, also during this preliminary information phase, the complainant was asked to identify the person who informed him on 12/17/2019 that several citizens had evidence of his absence from work and the withdrawal of firearms, as well as providing all the evidence he could have to prove these facts.

The reporting person did not respond to this request for information.

6. On 20/05/2021, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the City Council of (...) for an alleged infringement provided for in article 83.4.a) , in relation to article 32; all of them from 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 movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 05/25/2021.

7. The initiation agreement explained the reasons why no charge was made regarding the statement made by the person making the complaint, consisting of the fact that, on 12/17/2019, it was learned that different residents of the municipality had evidence that he was on leave from work, which had led to his firearms being taken away as a medical leave due to mental deficiencies.

In the present case, the reporting person did not provide the slightest indication that would allow this reported fact to be proven. In turn, the City Council certified that the file manager where the controversial file relating to the complainant was stored, in electronic form, only contained the accesses made by a single user, who was authorized by the exercise of their functions.

8. On 08/06/2021, the City Council of (...) made objections to the initiation agreement.

9. On 07/02/2021, the person instructing this procedure formulated a proposed resolution, by which it was proposed that the director of the Catalan Data Protection Authority admonish the City Council of (...) as responsible for an infringement provided for in article 83.4.a) in relation to the Article 32, both of the RGPD.

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

This resolution proposal was notified on 02/07/2021 and a period of 10 days was granted to formulate allegations.

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

proven facts

The City Council of (...) had not carried out, at least until 16/12/2019, a risk analysis to determine the appropriate technical and organizational measures to guarantee the security of the data it processed through the manager of files

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.

Apart from giving as reproduced the documents provided and the justifications made as part of the previous information, the City Council limited itself to stating in its statement of objections to the initiation agreement that, on 22/ 01/2020, carried out the necessary actions to guarantee the security of the data it handled through the file manager.

As stated in the preceding 4th, as part of the previous information, the City Council informed that on 01/22/2020, at its request, the Information and Communication Technologies Service of the Vallès Regional Council Oriental modified the category of users corresponding to the Citizen Security unit in the file manager, allowing access only to authorized users.

In relation to this and as indicated by the instructing person in the resolution proposal, it is necessary to highlight that the adoption of any measures to correct the effects of the infringement does not distort the imputed facts, nor does it change their legal qualification.

In the present case, however, the measures adduced by the City Council in its statement of objections to the initiation agreement also did not allow it to be considered that the effects of the imputed infringement had been corrected. Indeed, it should be noted that in the present sanctioning procedure it does not refer to the lack of any specific security measure, but to the fact of

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

not having carried out a risk analysis to determine the appropriate technical and organizational measures to guarantee the security of the data handled through the file manager.

3. In relation to the facts described in the proven facts section, it is necessary to refer to article 5.1.f) of the RGPD, which regulates the principle of integrity determined that personal data will be "treated in such a way that Adequate security of personal data is guaranteed, including protection against unauthorized or illegal processing and accidental loss, destruction or damage, through the application of appropriate technical and 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 the violation of "the obligations of the person in charge and of the person in charge in accordance with articles 8, 11, 25 to 39, 42 and 43", among which there is that provided for in article 32 RGPD.

4. 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."

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

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 a maximum period of 3 months from the day after the notification of this resolution, carry out a risk analysis in accordance with article 32 of the RGPD, to determine the appropriate technical and organizational measures to guarantee the security of the data it processes through the file manager.

Once the corrective measure described has been adopted, within the specified period, the City Council must inform the Authority within the following 10 days, without prejudice to the inspection powers of this Authority 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 article 32, both of the RGPD.

2. To require the City Council of (...) to adopt the corrective measures indicated in the 4th legal basis and accredit before this Authority the actions carried out by
fulfill them

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 the deadline

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

of one month from the day after its notification, in accordance with what they foresee 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,