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 112/2020, referring to the City Council of (...).

Background

1. On 20/04/2020, 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 personal data protection.
The complainant, an employee of the City Council, explained that approximately in December 2019, while she was on leave, the City Council "hired an external computer engineer and hacked my computer's password, accessing all the data that was inside, and leaving it without a password and with the data accessible to anyone who wants to enter since then, now four months ago. Inside the computer, apart from my personal data, there was a lot of other protected data (it had been 20 years since the justice of the peace of (...)) and other people's electronic signatures."

2. The Authority opened a preliminary information phase (no. IP 112/2020), 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 18/06/2020 the reported entity was required to report, among others, whether the computer assigned to the reporting person as an employee of the City Council. In the event of an affirmative answer, the City Council was required to report on the reasons for which the computer was accessed; the information that would have been accessed; as well as whether any measure had been implemented on the complainant's computer to prevent access by unauthorized persons.

4. On 18/06/2020, the City Council of (...) responded to the aforementioned request through a letter in which it stated the following:

- That the functions reserved for intervention secretary were carried out with character accidental by an employee (the reporting person).

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

- That following numerous and notorious irregularities detected in the exercise of the functions legally attributed to the complainant as accidental secretary-interventor, proceedings were initiated to proceed with the revocation of her accidental appointment, which concluded with the Decree of Mayor's Office dated 06/02/2020 resolving its revocation.
- That this fact has resulted in numerous actions by this person against the City Council of (...), criminal, contentious-administrative or various complaints.
- That the computer used by the complainant, which is a work tool owned by the City Council, is also the City Council's server and is, therefore, where the software must be installed in if necessary.

- That the reporting person was in a situation of temporary incapacity since 12/20/2019 and the City Council had to install and configure the instance of the SQL Server system and the ABSIS accounting software on the server, with the corresponding administrator powers.

- That on 14/01/2020 a technician from the IT company came and explained to the Mayor that to solve the problem it was necessary to reset the user's password.
- That a new user with Administrator permissions was created, with which the computer was started and the password could be reset.
- That the City Council accessed the server to install software, and in no case carried out a control task of the computer's content.
- That all the information necessary for the correct ordinary management of the municipal entity and the Court of Peace has been accessed, given that the person who performs the functions of secretary of the Court (who is not the person making the complaint, but a administrative assistant) needed access to this information in order to perform these functions.
- That said computer is protected, among others, by means of a password.

The reported entity attached various documentation to the letter, which was supplemented on 06/26/2020.

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.

2.1. About access to the computer.

In the present case, the complainant stated that the City Council of (...) breached his password and would have accessed the contents of his computer.

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

In this regard, the City Council has admitted that it accessed the computer assigned to the person reporting here, which was also the City Council's server, by creating a new user with administrator profiles.

This action is justified by the City Council on the fact that the complainant was on leave, that it was necessary to install certain software on the server and to access the necessary information to be able to continue with the management of matters that are the responsibility of the City Council and the Court of Peace.

Given the reasons invoked by the City Council, at the discretion of this Authority, it is considered that access to said computer or server was justified.

On the other hand, the complainant also stated that his computer was left without a password. However, the City Council has reported on several security measures implemented to protect the data stored on that computer, among which, precisely, there was password authentication.

2.2. On access to the data of the reporting person.

In relation to the statement made by the person reporting that the computer assigned to him contained his personal data, it is necessary to refer to Article 87 of Organic Law 3/2018, of December 5, on data protection personal data and guarantee of digital rights (hereinafter, LOPDGDD) which regulates the right to privacy and use of digital devices in the workplace. This precept determines that public employees have the right to the protection of their privacy in the use of digital devices made available to them by the employer (in this case, the City Council).

And the aforementioned article adds that the employer can access the content derived from the use of digital media provided to workers only for the purpose of monitoring compliance with labor or statutory obligations and to guarantee the integrity of the aforementioned devices.

Well, as part of the previous actions, the City Council was required to specify what information had been accessed, and in particular, whether strictly personal information of the person making the complaint had been accessed.

In response to said request, the City Council informed that only the information necessary for the correct ordinary management of the municipal entity and the Court of Peace was accessed. Therefore, according to the City Council, no access was made to private information that the person making the complaint could have stored there, beyond the documentation generated in the exercise of their work duties.

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

On the other hand, in its response the City Council also specified that the aforementioned computer was not accessed with the purpose of monitoring compliance with the work obligations assigned to the person making the complaint, but for the purposes that have been indicated in the right foundation 2.1 (install software on the server and access the information necessary for the development of its activity and that of the Peace Court).

For his part, the complainant has also not provided any further evidence or evidence to support his statements about possible access to his private information.

In short, from the preliminary information actions carried out by this Authority, no indication has been observed that allows us to infer that the City Council had accessed the private information that the reporting person could have stored on the computer assigned to him as an employee.

Consequently, the principle of presumption of innocence is applicable here given that it has not been possible to prove the existence of evidence of infringement and therefore administrative responsibility cannot be demanded. This principle, which is contained in article 53.2.b of the LPAC, recognizes the right "To the presumption of non-existence of administrative responsibility until the contrary is proven".

Aside from the above, it is considered pertinent to refer to the Authority's Recommendation 1/2013 on the use of email in the workplace, where it is advised that in the event of termination of the employment relationship, the the company facilitates the worker to obtain the private messages from the mail account, accessing the messages in the presence of the worker, in order to identify the messages of an exclusively personal nature.

Although said Recommendation refers only to e-mail, the guidelines contained therein are considered applicable to the present case and, consequently, given that from the information available it is inferred that the reporting person no longer provides services to the City Council can, if it deems it appropriate, address the City Council to request that it be given to him allow the access and/or deletion of strictly private (that is to say, non-professional) information stored on the assigned computer under the conditions set forth.

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:

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

1. File the actions of prior information number IP 112/2020, 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,