In this resolution, the mentions of the affected entity 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 entity, the physical persons affected could also be identified.

File identification

Resolution of sanctioning procedure no. PS 56/2022, referring to the City Council of (...)

Background

1. On 31/05/2022, 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 breach of the regulations on personal data protection .

Specifically, the person reporting stated that, in the exercise of his duties as a corporal of the Local Police of (...), on 11/15/2020, he had a telephone conversation with a worker of the Service d 'Medical Emergencies (hereafter, SEM), and denounces the fact that another corporal of the Local Police - with TIP (...)- accessed the record of the recordings of the telephone communications of the Local Police, downloaded the reference conversation on his personal telephone, and disseminated its contents to other officers and corporals in the corps.

In order to prove the facts, the complaint was accompanied by, among other documents, the Minutes of the Commission for the Prevention of Harassment (hereafter, CPA) of the City Council's Human Resources Service of (...), dated 03/23/2021, in which, following a complaint filed by the now complainant, the corporal with TIP (...) acknowledged having accessed the content of the conversation held between the now complainant and a worker of the SEM, denied having a copy of the conversation, and added that " *at that time (November 2020) everyone had access to the recordings of the calls, since the previous head of the Department (now retired) had given the keys to almost everyone in the prefecture. (...)".* The complaint was also accompanied by the Acts of the CPA in which the testimonies of the agents with TIP (...) and (...) of the City Council were collected, in relation to the facts that are now being reported. Of these witnesses, and in relation to the facts reported, the following statement recorded in the minutes signed by the agent (...)" stands out *that Mr.* [agent with TIP (...)] *commented publicly in a conversation that he had listened to a recording of a police intervention on November 15 in which Mr.* [now complainant] *proposed to the person he was talking to that he process a complaint against the colleagues of the police (...)".*

2. The Authority opened a preliminary information phase (no. IP 206/2022), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to 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 susceptible to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 13/06/2022 the reported entity was required to, among others, provide the access register to the telephone recordings made by the Local Police in the period between from November to December 2020, indicate the specific people who had credentials that allowed access to the telephone recordings recorded by the Local Police,

and argue the reasons why the agent with TIP (...) disclosed to certain agents the content of the telephone conversation held with the now complainant and an EMS worker.

4. On 06/28/2022, the City Council responded to the above-mentioned request in a letter stating the following:

- " *The City Council does not have the list of specific people, who provided service to the Local Police in the period November-December 2020, who had credentials (username and personal password) that allowed them access to the recordings telephone calls recorded by the Local Police. However, during the period November-December 2020, only certain corporals of the Local Police, including Mr.* [agent with TIP (...)] *, had an access code, provided by the previous chief of the Local Police, which currently does not provide services to the City Council of (...), for the exercise of entrusted professional attributions.*
- *We confirm that the chief inspector of the Local Police was one of the people who had the credentials to access the telephone recordings (...).*
- *The City Council does not have access to the recordings made by the Local Police, in the period between November and December 2020, given the time that has passed since the calls and registration are only stored for a period maximum of one month. After this period the data is deleted. (...)*
- *The telephone conversation with a worker of the Medical Emergency Service, in relation to a traffic accident, was not downloaded by the corporal, Mr [* agent with TIP (...)] *, but was only heard in the within the framework of the professional functions attributed to monitoring the service provided by the Local Police of (...) in the aforementioned traffic accident.*

Finally, the claimed entity explained that the Local Police had evidence that the members of the SEM requested by telephone explanations of " *the inadequate police assistance in the aforementioned accident* " and added that " *it was necessary the review of the conversation and in which it was found that the interlocutor of the Local Police who answered the call, the corporal* [now complainant], *acted incorrectly and not as expected of a corporal of the Local police. He verbalized negative evaluations of the Local Police service and made statements about a service performed by the Local Police in a traffic accident in which he had not participated. Likewise, he encouraged the Medical Emergency Service to file the corresponding report or complaint following the actions of the local police officers who intervened, including the corporal* [with TIP (...)], *in the service of accident assistance (...)".*

In the end, the City Council made it clear that the reasons for which access to the aforementioned telephone conversation was carried out, was none other than to know the reasons for which the SEM had asked for explanations from the Local Police , in relation to a certain incident.

5. On 07/22/2022, also during this preliminary information phase, the Authority's Inspection Area required the reported entity to provide a copy of the current risk analysis between the months of November 2020 and January 2021. Likewise, the City Council was required to report on which section of the specific document, analyzes the details of the activities that had to be subject to registration, in accordance with the National Scheme of Security (henceforth, ENS).

6. On 02/08/2022, and still within the framework of the prior information phase, the City Council of (...) responded to the aforementioned request, stating that it does not have a current risk analysis between the months of November 2020 and January 2021.

7. On 09/22/2022, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the City Council of (...) for three alleged infringements: two infringements provided for in article 83.4 .a) in relation to sections 1 and 2 of article 32, respectively; and, a third violation provided for in article 83.5.a) in relation to article 5.1 f); 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 circulation thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 09/23/2022.

8. The initiation agreement explained the reasons why no charge was made with respect to the fact reported, relating to the alleged download by the agent with TIP (...) of the conversation held by the reporting with an EMS worker, on her personal mobile phone. In summary, this fact was archived given that, apart from the statements of the now complainant, there was no other element that could corroborate that the agent downloaded the aforementioned conversation and save to your mobile device, download which, on the other hand, the City Council denied that it had occurred. In this respect, as this reported fact cannot be proven, the principle of presumption of innocence applies.

9. In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests.

10. On 10/10/2022, the City Council of (...) formulated objections to the initiation agreement , which are addressed in section 2 of the legal foundations.

11. On 15/12/2022, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish the City Council of (...) as responsible, for two violations provided for in article 83.4.a) in relation to paragraphs 1 and 2 of article 32.1, respectively; and a third violation provided for in article 83.5.a) in relation to article 5.1 f), all of them of the RGPD.

This resolution proposal was notified on 16/12/2022 and a period of 10 days was granted to formulate allegations.

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

proven facts

1. The City Council of (...) did not adopt the security and technical measures required in accordance with the ENS, which led to the fact that, for an indeterminate period, which at least includes the months of November and December 2020, the City Council did not know which people had the credentials that allowed access to the telephone recordings recorded by the Local Police, and did not keep the record of the people who accessed the referred telephone conversations one month after the completion of the call

2. The City Council of (...) during the months of November 2020 to January 2021 did not have the corresponding risk analysis, in relation to the personal data it handled.

3. The corporal of the Local Police with TIP (...) of the City Council of (...) publicly disseminated the content of the telephone conversation held by the now complainant with an employee of the SEM, without the City Council having accredited or justified that the people who became aware of the aforementioned information, following its dissemination by the corporal, were authorized to access the content of the recorded telephone recordings. This dissemination was carried out on an undetermined date, but after 11/15/2020, the date on which the aforementioned telephone conversation took place.

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 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.

2.1 About the fact tested first

The pleadings submitted on 10/10/2022, in the agreement to initiate the present procedure, highlighted the following considerations:

- That, regarding access to the content of the telephone recordings recorded by the Local Police, " *the system has a double authentication factor and an access key file is required to access it"* .

-That " *the previous inspector provided access permits to the telephone recordings recorded by the Local Police only to the corporals and, following the functions of monitoring the service provided by the Local Police of (...) in the traffic accident, Corporal (...) [TIP (...)] listened to the recording. This was motivated by the fact that members of the Medical Emergency Service had asked for an explanation of the inadequate police assistance in the traffic accident."*

- That *"following this action in the traffic accident and to avoid any type of incident with telephone recordings, as a preventive measure, the Local Police inspector decided to change the system of access permits to the recordings of the corporals. From then until now, the only person authorized to access the telephone recordings is the Inspector of the Local Police of the City Council of (...), who has access through user and password Likewise, the key file that allows the service to be launched is only installed on the desktop computer located in the office of the Local Police Inspector. This desktop computer is installed in Windows Server domain protected, both by user and password. In addition, access to the Police Inspector's office is protected with a key."*

Well, first of all, it should be noted that, as stated by the instructing person in the resolution proposal, the accused entity does not question the first of the facts alleged in this procedure,

referring to the lack of security and technical measures required of in accordance with the ENS. In fact, the Corporation admits that, following the reference incident, it was decided to change the system of access permissions to the telephone recordings, so that the only person authorized to access them is the Inspector of the Local police. In relation to the above, the City Council has also made it clear that the file that allows access to recordings of telephone conversations is only installed on the computer of the Local Police Inspector, in a Windows Server domain, protected by user and password, and that this computer is located in the Inspector's office, access to which is protected by a key.

According to the ENS, every organization must be able to clearly establish the traceability of access to personal data, in this case, to the recordings of telephone conversations (who, when, what information, etc.), something that did not happen in the case analyzed in which, as explained in the proven facts section, and argued in the resolution proposal, there was no record that collected this information. On the other hand, the City Council also did not guarantee that the credentials to access the system were always under the exclusive control of its users, which prevented it from being able to have certain information about the person or people accessing the data.

2.2 . About the fact tested second _

Given that the City Council has recognized the imputed facts, by means of a letter presented to the Authority on 02/08/2022 - precedent 6th - it is unnecessary to make any additional consideration in this regard, without prejudice to what will be said in the Foundation of law 3rd, on the legal qualification that these facts deserve.

2.3 About the fact third tested

Regarding the actions of the corporal of the Local Police with TIP (...) who publicly disseminated the content of the conversation held by the complainant here with an employee of the SEM, the accused entity argued the following:

- That *"the Corporal of the Local Police with TIP (...), (...), from the Town Hall of (...) accessed the recording of the call but there is no evidence that allow it to be asserted that he publicly disseminated the content of the conversation (...)"*

- That " *the action of the corporal (...)* [the complainant here] *(...), in relation to the conversation with the Medical Emergency Service following the traffic accident, was known by the members of the Local Police. However, this does not imply that the agents had access to the recording of the call and it cannot be ruled out that the corporal himself (...)* [the complainant here] was aware of it.

In summary, the City Council of (...) defended that there is no evidence to support the claim that the Local Police Corporal with TIP (...) disseminated the content of the telephone conversation to other officers, and adds since, it cannot be ruled out that they had access to it through the Corporal himself [here the complainant].

In relation to the above, it is appropriate to point out that, as transcribed in the first antecedent of this resolution, the minutes of the CPA of the Human Resources Service of the City Council of (...), dated 23/03/2021, collect the testimonies of agents with TIP (...) and (...) of the City Council, and in one of them - specifically the one signed by the TIP agent (...)- it

states literally that *"Mr. [agent with TIP (...)] commented publicly in a conversation that he had listened to a recording of a police intervention on November 15 in which Mr. [now complainant] proposed to the person he was talking to that he process a complaint against the colleagues of the police (...)"* . In this regard, it is also pertinent to point out that, in the preliminary information phase, the City Council did not question this fact.

In short, given the allegation of the denounced entity denying the existence of evidence to support the dissemination of the controversial information by the agent with TIP (...) to other agents, this The Authority cannot ignore the fact that, apart from the statements of the complainant here, there is a report of the CPA, signed by an officer of the Local Police, which confirms such dissemination; witness that, it should be noted, the accused entity has not misrepresented, neither in the previous information phase that preceded this sanctioning procedure, nor in the course of it.

For the above, the allegations made by the City Council cannot succeed.

3. In relation to the facts described in point 1 of the proven facts section, it is necessary to refer to article 5.1 f) of the RGPD, which regulates the principle of integrity and confidentiality, and determines that personal data *they* must be " *treated in such a way as to guarantee security data adequacy _ personal , including the protection against unauthorized or illegal treatment and against it loss , destruction or accidental damage , through the application of measures technical or organizational appropriate ".*

For its part, article 32.1 of the RGPD, regarding data security, provides the following:

> *"1. 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 severity for the rights and freedoms of natural 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, which if applicable includes, among others:*
> *a. Pseudonymization and encryption of personal data ;*
> *b. The ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services;*
> *c. The ability to quickly restore availability and access to personal data in the event of a physical or technical incident;*
> *d. A process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the safety of the treatment.*

In this respect, the first additional provision of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD) establishes the following:

> *"1. The National Security Scheme must include the measures that must be implemented in the event of processing of personal data to prevent their loss, alteration or unauthorized access, with the adaptation of the criteria of determination of risk in the processing of data as established in article 32 of Regulation (EU) 2016/769.*
> *2. Those responsible listed in article 77.1 of this Organic Law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of*

equivalent measures in companies or foundations subject to private law linked to those (...)."

The precepts transcribed establish the obligation of the data controller, in this case the City Council of (...), to adopt the appropriate security measures in order to guarantee a level of security appropriate to the risk.

For the case that concerns us here, it is necessary to take into account the security measures foreseen by the ENS, approved by Royal Decree 3/2010, of January 8, in force at the time of the commission of the facts. Specifically, articles 13, 14.1, 16 and 23 of the aforementioned ENS, provided for the following (the emphasis is ours):

Article 13. Risk analysis and management

1. *Each organization that develops and implements systems for the treatment of information and communications will carry out its own risk management.*
2. *This management will be carried out through the analysis and treatment of the risks to which the system is exposed. Notwithstanding the provisions of Annex II, some internationally recognized methodology will be used.*
3. *The measures adopted to mitigate or eliminate the risks must be justified and, in any case, there will be a proportionality between them and the risks.*

Article 14. Personnel management

(…)

4. *In order to correct, or demand responsibilities in their case, each user who accesses the system information must be uniquely identified, so that it is known, at all times, who receives access rights, what type they are, and who has performed a certain activity.*

Article 16. Authorization and access control

Access to the information system must be controlled and limited to duly authorized users, processes, devices and other information systems, restricting access to permitted functions.

Article 23. Activity register.

With the exclusive purpose of achieving the fulfillment of the object of this royal decree, with full guarantees of the right to honor, personal and family privacy and the own image of those affected, and in accordance with the regulations on protection and personal data , of public or labor function, and other provisions that apply, the activities of the users will be recorded, retaining the information necessary to monitor, analyze, investigate and document improper or unauthorized activities, allowing the person who acts to be identified at all times.

Likewise, it should be noted that Law 26/2010, of August 3, on the legal regime and procedure of the public administrations of Catalonia, in its eleventh additional provision, on the management of documentation and archiving of electronic documents, states the following:

"5. The information systems used by the public administrations included in the scope of application of this law must guarantee, whenever possible, the authenticity and integrity of their data, and also the traceability of the actions they carry to term".

During the processing of this procedure, the fact described in the first point of the proven facts section, consisting of the lack of adoption of the necessary technical and security measures , which is considered constitutive of the foreseen infringement, has been duly proven 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 pursuant to articles 8, 11, 25 to 39, 42 and 42"* , among which there is the provision in article 32.1 of the RGPD .

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

> *"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 of Regulation (EU) 2016/679."*

4. With regard to the fact described in point 2 of the proven facts section, regarding the failure to carry out a risk analysis, it is also necessary to refer to article 5.1.f) of the RGPD, transcribed in first point of the legal classification of the facts.

In turn, the second section of article 32 of the RGPD, in relation to risk analysis, establishes the following:

> *"2. When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the communication or unauthorized access to said data".*

Also article 28 of the LOPDGDD foresees the obligation of the person responsible for the treatment to adopt the appropriate technical and organizational measures in order to guarantee and certify that the treatment is in accordance with the RGPD, taking into account, in particular, the risks that are transcribed below:

> *"2. For the adoption of the measures referred to in the previous section, those responsible and in charge of the treatment must take into account, in particular, the higher risks that may occur in the following cases: a) When the treatment*
> *may generate situations of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of pseudonymization or any other significant economic, moral or social harm to those affected.*
> *b) When the treatment may deprive those affected of their rights and freedoms or may prevent them from exercising control over their personal data.*
> *c) When the non-merely incidental or accessory treatment of the special categories of data referred to in articles 9 and 10 of Regulation (EU) 2016/679 and 9 and 10 of this Organic Law or of data related to the commission of administrative infractions.*
> *d) When the treatment involves an evaluation of personal aspects of those affected with the purpose of creating or using personal profiles of them, in particular through the analysis or prediction of aspects related to their performance at work, their situation economic status, your health, your personal preferences or interests, your reliability or behavior, your financial solvency, your location or your movements.*
> *e) When data processing is carried out for groups of affected people in a particularly*

vulnerable situation and, in particular, for minors and people with disabilities.
f) When there is a massive treatment that involves a large number of affected or involves the collection of a large amount of personal data.
g) When personal data must be the subject of a transfer, on a regular basis, to third states or international organizations in respect of which an adequate level of protection has not been declared.
h) Any others that, in the opinion of the person in charge or the person in charge, may be relevant and in particular those provided for in codes of conduct and standards defined by certification schemes."

Well, in this case, the lack of risk analysis constitutes an infraction according to the provisions of article 83.4 of the RGPD which typifies as such, the violation of "the obligations of the manager *and the manager pursuant to the articles 8, 11, 25 to 39, 42 and 43 "* , among which there is the one provided for in article 32.2 RGPD.

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

"p) The processing of personal data without carrying out a prior assessment of the elements mentioned in article 28 of this Organic Law."

5. With regard to the conduct described in point 3 of the imputed facts, regarding the disclosure of the content of a telephone conversation, it is also necessary to refer to article 5.1 f) of the RGPD, transcribed in the first point of the qualification legal facts.

For its part, article 5 of the LOPDGDD, relating to the duty of confidentiality, provides:

"1. Those responsible and in charge of data processing as well as all the people who intervene in any phase thereof are subject to the duty of confidentiality referred to in article 5.1. f) of Regulation (EU) 2016/679.
2. The general obligation indicated in the previous section is complementary to the duties of professional secrecy in accordance with its applicable regulations.
3. The obligations established in the previous sections remain even if the relationship of the obligee with the person in charge or person in charge of the treatment has ended".

This imputed fact constitutes an infringement, according to the provisions of article 83.5 a) of the RGPD, which typifies as such, the violation of " *a) The basic principles for the treatment, including the conditions for the consent to tenor of articles 5,6, 7 and 9* ", among which there is the principle of confidentiality.

In turn, this conduct has been included as a very serious infringement in article 72.1 i) of the LOPDGDD in the following form:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679, infractions that involve a substantial violation of the articles mentioned therein and, in particular the following, are considered very serious and will be prescribed in three years: i) The violation of the duty of confidentiality established in article 5 of this organic law".

6. 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 . (...)".*

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 10 days from the day after the notification of this resolution, implement the corrective measures indicated below:

6.1 Regarding the facts described in the 1st point of the proven facts section, I certify that I have a log of access to the system that stores the recordings of the telephone conversations held by the Local Police.

6.2 With respect to the facts described in the 2nd point of the proven facts section, document the analysis of risks related to the treatments linked to the recording of the telephone calls of the Local Police and of the conversations held through the transmission equipment of the City Council.

Once the corrective measures described have been adopted, within the indicated deadlines, the City Council of (...) must inform the Authority within the following 10 days, without prejudice to its inspection powers Authority to carry out the corresponding checks.

With respect to the facts described in the 3rd point of the proven facts section, the adoption of corrective measures should be ruled out since it is a specific and consummated fact.

For all this, I resolve:

1. Admonish the City Council of (...) as responsible for three violations: two violations provided for in article 83.4.a) in relation to sections 1 and 2 of article 32, respectively; and, a third violation provided for in article 83.5.a) in relation to article 5.1.f), all of them of the RGPD.

2. To require the City Council of (...) to adopt the corrective measures indicated in the 6th legal foundation and to accredit before this Authority the actions taken to comply with 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 one month from the day after its notification, in accordance with the provisions of 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,