IAI 2/2021

Report issued at the request of the Commission for the Guarantee of the Right of Access to Public Information in relation to the claim presented against a city council for the denial of access to information on professional contacts and emails

The Commission for the Guarantee of the Right of Access to Public Information (GAIP) asks the Catalan Data Protection Authority (APDCAT) to issue a report on the claim presented against a City Council for the denial of access to information on professional contacts and e-mails.

Having analyzed the request, which is accompanied by a copy of the administrative file processed before the GAIP, and in accordance with the report of the Legal Counsel, I issue the following report:

Background

1. On December 13, 2019, a person who has been working as a chief sergeant in the Local Police of the City Council (...) presents to this corporation an instance of access to information in the following terms:

> *"I explain: On date (...) I completed the service commission at the City Council (...) as Sergeant-in-Chief of the Local Police. That access to my corporate email has been blocked (...), that due to this issue I have all the contacts of organizations, ISPC, Chiefs of Police and commands, service companies, etc., to whom I do not I have not been able to communicate my departure or have the contacts to be able to communicate with them.*
> *Request: To be able to access or recover mail and mail information (...)."*

2. On February 11, 2020, this same person presented to the APDCAT a letter of complaint against the City Council for neglecting the right of access to their personal data.

3. On September 15, 2020, the director of the APDCAT issues a resolution of the rights protection procedure brought against the City Council, in the following terms:

> *"First.- Partially estimate the guardianship claim made by Mr. (...) against the City Council (...), and recognize the right of this person to access his private emails that he sent or received through the his corporate e-mail from the City Council, to the e-mails he received relating to his payroll, as well as to the information relating to his private contacts, corresponding to the period of time he exercised in the services commission the functions of sergeant-in-chief of the Local Police of this City Council. Dismiss the claim with regard to the rest of the information requested, for the reasons indicated in legal basis 4.2."*

4. On October 8, 2020, this person presents a new instance before the City Council in which, in accordance with legal basis 4.2 of the APDCAT resolution cited in the previous point, he requests:

"According to art. 18 LTC I request access to professional data: (emails, contacts, etc.), from the mail (...)."

5. On November 26, 2020, the GAIP forwards the claim to the City Council, informing it of the processing of the mediation procedure at the express request of the complaining party, and requiring it to issue a report on which they base their positions, as well as the complete file relating to the request for access to public information, the identification of the third parties who are affected by the requested access, as well as the person or persons who will represent at the mediation session.

6. On January 13, 2021, the GAIP requests this Authority to issue the report provided for in article 42.8 of Law 19/2014, of December 29, on transparency, access to public information and good government, in relation to the claim presented.

Legal Foundations

I

In accordance with article 1 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, the APDCAT is the independent body whose purpose is to guarantee, in the field of the competences of the Generalitat, the rights to the protection of personal data and access to the information linked to it.

Article 42.8 of Law 19/2014, of December 29, on transparency, access to public information and good governance, which regulates the claim against resolutions on access to public information, establishes that if the refusal has been based on the protection of personal data, the Commission must issue a report to the Catalan Data Protection Authority, which must be issued within fifteen days.

For this reason, this report is issued exclusively with regard to the assessment of the incidence that the requested access may have with respect to the personal information of the persons affected, understood as any information about an identified or identifiable natural person, directly or indirectly, in particular through an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of physical, physiological, genetic, psychological, economic, cultural or social security of this person (article 4.1 of Regulation 2016/679, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free circulation of such data and by which repeals Directive 95/46/EC (General Data Protection Regulation, hereafter RGPD).

Therefore, any other limit or aspect that does not affect the personal data included in the requested information is outside the scope of this report.

The deadline for issuing this report may lead to an extension of the deadline to resolve the claim, if so agreed by the GAIP and all parties are notified before the deadline to resolve ends.

Consequently, this report is issued based on the aforementioned provisions of Law 32/2010, of October 1, of the Catalan Data Protection Authority and Law 19/2014, of December 29 , of transparency, access to public information and good governance.

In accordance with article 17.2 of Law 32/2010, this report will be published on the Authority's website once the interested parties have been notified, with the prior anonymization of personal data.

II

The object of the complaint is, as can be seen from the statements of the complaining party and the set of information contained in the file, access to the contacts and professional e-mails of the corporate e-mail that the person making the claim had while working in the services commission the functions of chief sergeant of the Local Police of the City Council (...).

Article 4.2) of the RGPD considers *"treatment": any operation or set of operations carried out on personal data or sets of personal data, either by automated procedures or not, such as collection, registration, organization, structuring, conservation , adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of enabling access, comparison or interconnection, limitation, deletion or destruction."*

The RGPD provides that all processing of personal data must be lawful (Article 5.1.a)) and, in this sense, establishes a system of legitimation of data processing that is based on the need for one of the legal bases established in article 6.1 to apply. Specifically, section c) provides that the treatment will be lawful if *"it is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment".*

Article 6.3 of the RGPD establishes that the basis of the treatment indicated in this article 6.1.c) has to be established by the Law of the European Union or by the law of the Member States that applies to responsible for the treatment.

The referral to the legitimate basis established in accordance with the internal law of the Member States concerned reference this article requires that the development norm, when dealing with the protection of personal data of a fundamental right, has the status of law (Article 53 EC), as it has come to recognize article 8 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD).

For its part, article 86 of the RGPD provides that *"personal data from official documents in the possession of some public authority or public body or a private entity for the performance of a mission in the public interest may be communicated by said authority, organism or entity in accordance with the Law of the Union or of the Member States that they are applied in order to reconcile public access to official documents with the right to protection of personal data under this Regulation."*

Law 19/2014, of December 29, on transparency, access to public information and good governance (hereafter, LTC), aims to regulate and guarantee the transparency of public activity.

Article 18 of the LTC recognizes the right of people to *"access public information, which does reference article 2.b, in an individual capacity or in the name and representation of any legally constituted legal person" (section* 1).

Article 2.b) of the LTC defines "public information" as *"the information prepared by the Administration and that which it has in its power as a result of its activity or the exercise of its functions , including that supplied by the other obliged subjects in accordance with the provisions of this law".*

Professional emails sent and received by the person claiming through their account corporate email during the period in which he performed the functions of chief sergeant of the Local Police, as well as the email addresses of professional contacts, is information that is in the possession of the City Council as a result of the exercise of the functions police officers assigned to the person claiming Therefore, it is public information for the purposes of article 2.b) of the LTC and, consequently, subject to the regime of the right of access (article 18 LTC).

This right of access, however, is not absolute and may be denied or restricted for the reasons expressly established in the laws. Specifically, and with regard to the right to the protection of personal data, it is necessary to take into account the limitations and criteria provided for in the transparency legislation (articles 23 and 24 LTC), and the principles of the personal data protection regulations.

III

On the one hand, the claimant requests access to the e-mail addresses of his professional contacts, which are in the possession of the City Council, having blocked his corporate e-mail account due to the termination of the service commission in this council.

As this Authority has previously highlighted (for example, in reports IAI 35/2020 or in CNS opinion 4/2011, available on the website https://apdcat.gencat.cat/ca/inici), work or professional email addresses that can be associated with identifiable natural persons (article 4.1 RGPD) must be considered as personal data.

That being the case, with respect to the requested access, the provisions of article 24 of the LTC will apply:

> *"1. Access to public information must be given if it is information directly related to the organization, operation or public activity of the Administration that contain merely identifying personal data unless, exceptionally, in the case specific should the protection of personal data or other constitutional rights prevail protected*
>
> *2. If it is other information that contains personal data not included in article 23, it can give access to information, with the previous reasoned weighting of the public interest in the disclosure and the rights of the affected persons. To carry out this weighting, to take into account, among others, the following circumstances:*
> *a) The elapsed time.*

b) The purpose of the access, especially if it has a historical, statistical or scientific purpose, i the guarantees offered.
c) The fact that it is data relating to minors.
d) The fact that it may affect the safety of people.
(...).”

At the outset, the applicability of what is established in section 1 must be ruled out, given that in the case that we occupies the requested data is not merely identifying data, but it is one
contact information In addition, they would not only affect personnel in the service of the administration, but could also affect other people.

Paragraph 2 of this article will therefore apply, and it will be necessary to carry out one
weighting between the public interest in its disclosure and the consequences that this may have on it right to data protection of those potentially affected.

A first element to take into account in this regard is that, according to the information available, the contact details requested refer to people with whom the same claimant would have had a professional relationship during the period of time in which he served as Chief Sergeant of the Local Police.

The previous existence of this professional relationship between the person making the claim and the people affected by the access, maintained through the respective corporate email accounts, makes any expectation of privacy that these people may have regarding the disclosure of this data disappear personal by the City Council to the now claimant. Not only would it be personal information known to the person making the claim, but the affected people would be
fully aware of this circumstance.

Given this, it can also be assumed that, at least in many cases, we will find ourselves in front of personal data related or linked to the professional activity carried out by the people affected by the access (corporate or work email address), so a priori their private sphere should not be affected.

Another element to consider is the purpose of the access. Article 18.2 of the LTC provides that the exercise of the right of access is not conditioned on the concurrence of a personal interest, and is not subject to motivation nor does it require the invocation of any rule. However, for the purposes of the weighting of Article 24 of the LTC, knowing the motivation for which the claimant wishes to access the information may be a relevant element to take into account.

In the present case, the claimant states in his request that, following the blocking of the corporate email account by the City Council, *"I have all the contacts of organizations, ISPC, Chiefs of Police and Commands, service companies , etc., to whom I have not been able to communicate my departure or have the contacts to be able to communicate with them".*

It is clear from these statements that the aim of the claimant's access is to be able to get in touch with the people with whom he has had a professional relationship
as chief sergeant of the City Council's Local Police, for the purposes of informing them of the termination of their employment relationship with this City Council, on whose behalf they have maintained such a relationship.

It can be said, therefore, that we would be faced with the use of professional data (work mail) for purposes that could also be qualified as professional or work, on the understanding that this would be the last professional communication that would be maintained with these people as an employee of the City Council (end of their professional relationship).

In view of these circumstances, in the present case the claimant's right to access the e-mail addresses of his professional contacts as requested could be recognized.

This is without prejudice to the fact that at the time of delivering this data it is convenient to remind the person claiming the applicability of the data protection regulations to the subsequent processing of this information (article 15.5 of *Law 19/2013, of December 9, de transparencia, acceso a la información pública y buen gobierno* (LTC)), particularly the principle of purpose limitation (article 5.1.b) RGPD), so any other treatment that could be carried out other than what would justify the 'access to data (inform your professional contacts that you no longer work as a sergeant-in-chief of the Local Police) could be contrary to data protection regulations.

IV

On the other hand, the claimant also requests to be able to recover the content of all the professional e-mails that he sent or received through his corporate e-mail corresponding to the period of time that he performed the duties of sergeant-in-chief of the Local Police in the service commission.

It must be taken into consideration that the corporate e-mail constitutes, like the rest of the computer resources, a work tool that the City Council makes available to the staff for the development of the tasks and functions entrusted to it. In this sense, it constitutes a basic tool for internal and individual communications with the people with whom this staff maintains relations by virtue of the powers attributed to it.

In the present case, the content of the emails to which access is sought is related to the tasks that the claimant carried out as chief sergeant of the Local Police. In other words, they contain professional information linked in any case to the local administration's own activity in this area of municipal action. This information may not only refer to the person making the claim and/or to the sender/ receiver of the e-mail, but mainly to third parties.

In general, it is the duty of a local police sergeant to direct and supervise the police actions of the personnel in his charge in accordance with the guidelines set by his superiors, with the procedures established by the corporation and current legislation, as well as coordinating the system administrative, and, in any case, the performance of the police functions defined in Law 16/1991, of July 10, of the local police.

Despite not having the specific content of these emails, in view of the functions that current legislation attributes to the Local Police, we are faced with information that may be of a different nature and affect to a greater or lesser degree the privacy of the people it refers to.

Thus, it must be taken into consideration that the content of these emails may contain special categories of data (Article 9 RGPD) or data included in this category with a specific regime, such as those relating to administrative or criminal offences.

Article 23 of the LTC states that *"requests for access to public information must be denied if the information sought contains particularly protected personal data, such as those relating to ideology, trade union affiliation, religion, beliefs, racial origin, health and sex life, and also those relating to the commission of criminal or administrative offenses that do not entail a public reprimand to the offender, unless the affected party expressly consents to it by means of a written document that must accompany the request."*

For its part, article 15.1, paragraph two, of the LT establishes that *"if the information includes personal data that refers to racial origin, health or sex life, includes genetic or biometric data or contains relative data to the commission of criminal or administrative infractions that did not entail a public reprimand to the offender, access may only be authorized if the express consent of the affected person is obtained or if the latter is protected by a rule with the force of law."*

The claimant's access and obtaining a copy of the professional emails containing this type of personal data, once their employment relationship with the City Council has ended, should in any case be limited on the basis of what the cited articles provide.

But beyond that, the content of these professional emails may also contain data deserving of a special reservation or confidentiality in view of the concurrence of certain qualified circumstances (for example, situations of social vulnerability, data of minors, data related to gender violence, etc.) or in attention to the nature of the matters dealt with by the person making the claim as a result of their police activity or in the exercise of assigned police functions.

In addition, it cannot be ruled out that the intended access could affect a large volume of people. Although the number of people affected is not actually a decisive criterion when it comes to being able to limit access, it must be taken into account that when the people affected are very numerous, this can lead to a series of problems in being able to attend to the sun request for access with the appropriate guarantees, in particular, grant the hearing procedure provided for in article 31 of the LTC and assess, case by case, whether the protection of personal data or the right to access of the person claiming.

A reasoned weighting between the different rights and interests at stake that must be done in accordance with article 24.2 of the LTC, requires taking into account this circumstance that may lead to a denial of access to this information in the event of no the relevance that it may have for the person claiming to have this information is sufficiently proven.

It is certainly not mandatory, as stated, to include in the application the reasons for which access is sought (articles 18.2 and 26.2 LTC) but, failing to do so, this element cannot be taken into account in when assessing the different rights and interests at stake.

In this case, it must be said that the person making the claim does not adduce any specific reason why he wants to access the contents of the set of professional emails in the corporate email account provided to him by the City Council for the exercise of his duties as a sergeant in chief

Given this, access should be understood as framed within the purpose of the transparency law itself. According to its article 1.2, the purpose of the LTC is *"to establish a system of relationship between the people and the public administration and the other obliged subjects, based on the knowledge of the public activity, the incentive of the citizen participation, the improvement of the quality of public information and administrative management and the guarantee of accountability and responsibility in public management."*

Given these circumstances, it does not appear to be justified, from the point of view of data protection, the obtaining in a generalized way by the person claiming a copy of the set of professional e-mails as requested.

This, without prejudice to the fact that in some specific case the access and obtaining a copy of certain e-mails could be justified in view of the specific circumstances or reasons that the person making the claim can allege (for example, in the case of dealing with se of information necessary for your right of defence).

conclusion

The right to data protection does not prevent the claimant from being given the email addresses of their professional contacts. On the other hand, based on the information available, it would not be justified for the claimant to obtain a copy of the set of professional emails that he sent or received through his corporate email corresponding to the period of time he worked in services commission the functions of chief sergeant of the Local Police.

Barcelona, February 4, 2021