apdcat
Autoritat Catalana de Protecció de Dades

Legal report issued at the request of the Commission for the Guarantee of the Right of Access to Public Information in relation to the claim against the refusal by a City Council to request access to disciplinary records of the local police

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 a claim submitted in relation to the refusal by a City Council to request for access to disciplinary records of the local police.

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 Adviser, I issue the following report:

Background

1. On February 23, 2023, a person submits an application to a City Council in which he requests *" a copy of all the files disciplinary and procedures of information reserved for members of the body of the Urban Guard [...] that are there resolved the years 2020, 2021 and 2022".*

2. On March 1, 2023, the City Council decides to deny the request for access, ultimately, considering that it affects specially protected data provided for in the transparency regulations and the applicant has not accompanied the express consent of the people affected.

3. On March 6, 2023, the applicant submits a new request to the City Council in which he requests *"[...] a copy of the disciplinary files and reserved information that have been resolved during the years 2020, 2021 and 2022, and the resolution of these".*

The requesting person adds the following: *" I am asking for the files that have already been resolved and not those that are being processed, so that it cannot be argued that the knowledge or the disclosure of the information entails a detriment to the investigation or the sanction of criminal, administrative or disciplinary offences. Nor can it be considered to be particularly protected personal data if the files are delivered anonymously."*

4. On March 10, 2023, the City Council decides to estimate the request for access:

"FIRST. Accept the request for access to public information presented by [...], with the understanding that the requested documentation will be provided anonymized .

SECOND Urge the Department of Human Resources to, as soon as possible, provide in electronic format and duly anonymized , the information relating to the confidential and disciplinary files of the Guardia Urbana, resolved in the years 2020, 21 and 22 or in case if they do not have this documentation, they will formally communicate it."

5. On May 3, 2023, the applicant submits a claim to the GAIP in which he reiterates the terms of his application and states that the City Council has not executed the resolution dated March 10 for the which estimated access to the requested information.

6. On May 11, 2023, the GAIP sends the claim to the City Council, and asks for a report setting out the factual background and the basis for its position in relation to the claim, as well as the complete file and, if applicable , specifying the third parties affected by the claimed access.

7. On June 8, 2023, the GAIP requests a report from this Authority, in accordance with the provisions of article 42.8 of Law 19/2014, of December 29, on transparency, access to public information and good government

8. On June 12, 2023, the GAIP sent this Authority the report and file presented by the City Council in response to the request of the GAIP dated May 11, 2023. According to the file, this report issued by the Human Resources department, at the request of the City Council's transparency, access to information and good governance department.

In particular, the City Council informs that the human resources department, upon reviewing the claim submitted to the GAIP, considers that access to the requested information cannot be granted because it contains information relating to the commission of administrative infractions which is not it can be provided even if it is previously anonymized , in the absence of the express written consent of the affected persons.

The City Council also bases its refusal to provide this documentation on the understanding that it affects public security, because *"[...] police protocols, planning of fundamental services to guarantee the integrity of citizens, internal information relevant to security and crime prevention and aspects protected by professional secrecy. The operation of the Urban Guard is reflected daily in the reports, plans, orders, e-mails, and many other documents in which the details of their activity are included, details that, if made available to anyone who asked for it, would provide information that could hinder or prevent the good functioning of police activities, both preventive and executive [...]".*

And, finally, at the conclusion of the report, the City Council refers to the fact that *"[…] data could only be given at a statistical level such as the number of reserved information opened, closed, disciplinary proceedings initiated, how many of these are minor infractions, how many are serious, etc. All this without prejudice to the fact that the GAIP can be consulted to clarify this issue"*

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 complaints against resolutions regarding access to public information, establishes that if the refusal has been based on the protection of personal data, the Commission must request a report from 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 (art. 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 Directive 95/46/CE (General Data Protection Regulation, hereafter RGPD) is repealed.

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.

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 data protection regulations, in accordance with what is established in articles 2.1 and 4.1) of the RGPD, apply to the treatments that are carried out on any information " *on an identified or identifiable natural person ("the interested party »); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a number, an identification number, location data, an online identifier or one or more elements of identity, shall be considered an identifiable physical person physical, physiological, genetic, psychological, economic, cultural or social of said person* ".

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* .

In accordance with the provisions of article 5.1.a), any processing of personal data must be lawful, loyal and transparent in relation to the interested party and, in this sense, the RGPD establishes the need to participate in some of the legal bases of article 6.1, among which section c) provides for the assumption that the treatment " *is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment* ".

As can be seen from article 6.3 of the RGPD and expressly included in article 8 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), the processing of data can only be considered based on these legal bases of article 6.1. c) and e) of the RGPD when so established by a rule with the rank of law.

For its part, article 86 of the RGPD provides that " *the personal data of official documents in the possession of any 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 applies to them in order to reconcile the public's access to official documents with the right to the protection of personal data under this Regulation* .

Public access to documents held by public authorities or public bodies is regulated in our legal system in Law 19/2014, of December 29, on transparency, access to public information and good governance (hereinafter, LTC) , which recognizes people's right of access to public information, understood as such " *the information prepared by the Administration and that which it has in its power as a result of its activity or the "exercise of his functions, including that supplied by the other obliged subjects in accordance with the provisions of this law* " (article 2.b) and 18 LTC). State Law 19/2013, of December 9, on transparency, access to public information and good governance (hereafter, LT), is pronounced in similar terms, in its articles 12 (right of access to public information) and 13 (public information).

In the case we are dealing with in which access is requested to certain files sent by the City Council, this information must be considered public for the purposes of article 2.b) of the LTC and subject to the right of 'access (article 18 of the LTC), being documentation in his possession as a result of his activity.

III

The claimant is seeking access to the classified information and disciplinary files of the local police in the time period between 2020 and 2022 that have already been resolved (hereinafter, the files).

Article 55 of Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations (henceforth, LPAC), establishes that prior to the start of the procedure, the body competent authority may open a period of information or prior actions in order to know the circumstances of the specific case and the convenience or not of starting the procedure.

At the same time, article 14.1 of Decree 179/2015, of August 4, which approves the Regulation of the procedure of the disciplinary regime applicable to the local police forces of Catalonia, establishes the following:

"14.1 Before initiating a disciplinary procedure, the body competent to initiate it may, on an optional basis, initiate preliminary proceedings with the nature of confidential information, to clarify the events that occurred as well as the alleged responsible parties. Subsequently, the instructor must agree that this information is included in the disciplinary file.
[...]"

It is a consolidated jurisprudential criterion that the investigation phase prior to the start of a procedure does not properly constitute an administrative procedure (among others, STSJM 471/2006, of May 24), as well as that its reserved nature prevents that during its processing access to its content can be facilitated given that knowledge of it may entail a clear detriment to the result of the same (among others, STS 21/2018, of February 15).

Along these lines, the LTC expressly establishes the possibility of limiting or denying access to public information if its knowledge or disclosure entails a detriment to the investigation or sanction of the criminal, administrative or disciplinary offense in question (article 21.1.b)).

Thus, the right of access to this documentation, even in the case that the intended access was to own data (art. 15 of the RGPD), could be limited during the investigation actions and whenever consider that it may prejudice the investigation of conduct that could be sanctioned administratively or even criminally (limitation provided for in article 23.1.d) of the RGPD). In short, this limitation would affect any person affected by the actions, regardless of the position they hold.

In the case at hand, however, the claimant has specified that he is only interested in accessing the files that have already been resolved. Thus, it should be borne in mind that once the previously reserved information phase has been concluded with the adoption of a decision, either with the archive of actions or with the agreement to initiate disciplinary proceedings, probably already the limit provided for in article 21.1.b) of the LTC does not apply and it is necessary to analyze whether any other limitations of those established in the LTC apply.

On the basis of what has been explained, it is appropriate to place the limits established in the LTC relating to the protection of personal data, that is to say, the provisions of article 23 and 24 of the LTC.

Article 23 of the LTC provides the following:

"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 sexual 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 by means of a written which must accompany the application".

In the event that the intended access does not affect particularly protected personal data referred to in article 23 of the LTC, it is necessary to comply with the provisions of article 24 of the LTC, which provides for the Next:

"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 contains merely identifying personal data unless, exceptionally, in the specific case it has to prevail over the protection of personal data or other constitutionally protected rights.

2. If it is other information that contains personal data not included in article 23, access to the information can be given, with the previous reasoned weighting of the public interest in the

disclosure and the rights of the people affected. To carry out this weighting, the following circumstances must be taken into account, among others:

a) The elapsed time.

b) The purpose of the access, especially if it has a historical, statistical or scientific purpose, and the guarantees offered.

c) The fact that it is data relating to minors.

d) The fact that it may affect the safety of people.

3. Requests for access to public information that refer only to the applicant's personal data must be resolved in accordance with the regulation of the right of access established by the data protection legislation staff".

Based on these forecasts, the analysis of access to all the files will be carried out globally, taking into account the categories of people who can predictably be affected, since the specific content of the files affected by the sun is unknown · request for access, and the fact that the City Council has not provided information about the people affected in the case of a claim for access to public information before the GAIP.

In this sense, it is clear that the access request affects public employees whose data appear in the requested documentation following the exercise of their intervention in the processing of the previous information and, where appropriate, disciplinary files, as well as the alleged person(s) responsible for the infraction. At the same time, it is possible that in some cases whistleblowers and other people such as witnesses may be affected.

IV

At the outset, it must be agreed that access to the data of public employees who are affected by the request for access is due to the exercise of their functions, such as their intervention in the processing of files, it must be analyzed from the point of view of what is provided for in article 24.1 of the LTC, that is, *"Access must be given to public information if it is information directly related to the "organisation, operation or public activity of the Administration that contains merely identifying personal data unless, exceptionally, in the specific case the protection of personal data or other constitutionally protected rights must prevail".*

At the same time, it is necessary to take into account article 70.2 of Decree 8/2021, of February 9, on transparency and the right of access to public information (RLTC), which provides for the following:

"For the purposes of what is provided for in article 24.1 of Law 19/2014, of December 29, personal data consisting of the name and surname, the position or position held, body and scale, the functions performed and the telephone and addresses, postal and electronic, of professional contact, referring to staff in the service of public administrations, senior positions and managerial staff in the public sector of public administrations.

In cases where the publication or access to an administrative document requires the identification of the author, the location data, the number of the national identity document or equivalent document must be removed in particular and the handwritten signature. If the signature is electronic, the electronically signed document must be published in such a way that the properties of the electronic certificate used for the signature cannot be accessed.

The location data must be deleted in the case that it is not merely identifying data of the author in his position of position or staff in the service of public administrations".

Thus, with regard to the identification data (name and surname and position) of the public employees who have intervened in the exercise of their functions within the framework of the processing of the files to which access is requested, or data identifiers of the public employees who had intervened in the different procedures being investigated, as long as their actions are not directly related to the alleged irregular conduct that has been investigated, the claimant's access to this data must estimated on the basis of article 24.1 of the LTC, unless there is an exceptional circumstance for the affected person (for example, being in a situation of special vulnerability).

With regard to access to the identity of whistleblowers, if applicable, the analysis of the possibility of access must be carried out through the weighting between the public interest in the disclosure of this information and the rights of these persons under the terms of article 24.2 LTC.

One of the elements to carry out the weighting is the purpose of the access . To this end, it should be borne in mind that 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, does not remain subject to motivation nor does it require the invocation of any rule Now, for the purposes of weighting, knowing the motivation for which the person making the claim wishes to access the information can be a relevant element to take into account.

However, the file sent does not state the purpose for which the claimant seeks access to the files. Consequently, it is necessary to analyze the possibility of access from the perspective of the general purpose of the transparency regulations, that is to say, the possibility of offering tools to citizens for the control of the actions of the public authorities. And, from the point of view of this purpose, it does not seem that in the case like the one raised, there is a special public interest in disclosing the identity of the complainants. The principle of data minimization (art. 5.1.c) of the RGPD), according to which the personal data provided must be adequate, relevant and limited to what is necessary for the intended purpose, would prevent also in this case access to said information.

In any case, with more reason it is necessary to limit access to specially protected data referred to in article 23 of the LTC (including data on health, those relating to ideology, religion, beliefs or racial origin), unless the consent of the affected persons is available or one of the presuppositions referred to in article 15 of the LT is met.

Regarding other people who may be affected by the access request, a priori the same conclusion must be reached, that is to say, it does not appear from the file sent that there is a special public interest in the disclosure of the identity of these people and, consequently, it is necessary to limit their access.

v

Regarding the information relating to the alleged offenders or offenders contained in the previous investigation and, where appropriate, subsequent initiation of the disciplinary procedure, it should be borne in mind that this Authority has maintained that this information is related to the commission of infractions criminal or administrative in respect of which article 23 of the LTC, among other categories of data, establishes the denial of access except in the case of a public warning to the offender, or express consent is available of the affected

In relation to this issue, the GAIP did not consider these categories of data included in resolution 1097/2021, of December 16, changing the criteria it had been following in relation to this issue. However, this Authority reiterates its position, which is included, among others, in the IAI 2/2022 report (available on the APDCAT website www.apdcat.cat) . In particular, this report considered the following:

"[...] The Public Administration is endowed by the legal system with administrative powers, among which is the sanctioning power or ius puniendi , that is, the power to impose certain sanctions when an administrative offense has occurred (art. 25.1 of the Spanish Constitution).

Reference should be made to Constitutional Court ruling 66/1984, of June 6 (and, before that, STC 2/1981, or 81/1983), which distinguishes between two categories of administrative sanctions: those that protect order general and those that pursue the self-protection of the administrative apparatus and that are the result of a special relationship of subjection, among which includes those of a disciplinary nature.

Although the distinction is somewhat imprecise, the Constitutional Court has been specifying material criteria that facilitate this differentiation. Thus, he has considered that the relations of special subjection are situations from which the citizen integrates into a pre-existing institution that projects its authority over him, apart from his common condition as a citizen, and the fact of acquiring a specific status of individual subject to a public power that is not common to all citizens, as well as that this relationship must be inserted in the organization of public services (SSTC 2/1987, 42/1985, 50/2003 and 81/2009).

The sanctioning power that protects the general order can affect various spheres of life (such as public order, traffic, urban planning, etc.), and all citizens can be active subjects In accordance with the aforementioned sentence of the Constitutional Court, these sanctions are "[...] close to the punitive and demanding ones, in line of principles, of guarantees that, having their initial field of application in the punitive, are extensible to the sanctioner [...]"

With regard to administrative sanctions resulting from a special relationship, as would be the case with disciplinary ones, the Administration only seems to pursue its own protection as an organization or institution, with respect to those directly related to it. According to STC 66/1984, these sanctions are "[...] established for cases of transgression of the obligations included in the regulations applicable to the case and assumed voluntarily [...], sanctions that, in the exercise of a power inserted in the table we have discussed, correspond to the actions of the Administration within the legal framework established for the effect and with submission to the ends that justify them and that, within the consecration of the full submission of the Administration to jurisdictional control in the terms defined today in article

106 of the Constitution, guarantee the jurisdictional protection of the hypothetical transgressor ".

In the case of disciplinary proceedings concerning personnel of public administrations, it must be taken into account that disciplinary proceedings in respect of their workers processed by public administrations are part of their sanctioning power, in this case in respect of their own workers, for the commission of disciplinary administrative infractions. As can be seen from article 94 of the Basic Statute of the Public Employee (EBEP), approved by Royal Legislative Decree 5/2015, of October 30, and as recognized by jurisprudence (among others STS of July 3, 2012, FJ 6) disciplinary procedures must conform, with some nuance, to the general principles of administrative sanctioning law.

[...]

It seems clear, therefore, that we are dealing with the exercise of an administrative power in the exercise of a public function of the professional associations, which must be subject to the principles of the ius punishment of the administration, and to which the same guarantees must be applied by the affected persons. That being so, it would not seem justified to deprive persons sanctioned under a disciplinary scheme which forms part of a public function from the provisions of Article 23 LTC.

But in addition, if we analyze them from the point of view of the impact that the disclosure of this type of information can have on the private lives of the people affected, there also does not seem to be any reason to make a distinction that leads to the exclusion of disciplinary sanctions from what is established in article 23 LTC.

It should be taken into account (that) the categories of data that were included in Article 15.1 LT and Article 23 LTC, led to the data that were provided as specially protected in Article 7 of Organic Law 15 /1999, of December 3, on the protection of personal data (LOPD), which included in the category of specially protected data the data relating to the commission of criminal or administrative offenses (7.5), which granted a protection especially for administrative offences. And the truth is that the reasons that led to granting administrative sanctions a special protection are fully applicable to disciplinary infractions.

It is obvious that the disclosure of administrative offenses can reveal information about a person's conduct, or better, about aspects of his conduct that have given rise to a reprimand. In certain cases, it is the legal system that provides for the disclosure of the sanctions imposed (in the case of sanctions consisting of a public reprimand or other cases in which the publication of the sanction is foreseen). But outside of these cases, it should be borne in mind that the disclosure of this type of information can lead to a significant interference in the right to data protection in terms of its public image and, especially, due to the risks of discrimination or stigmatization that may occur in different areas (social, professional, work, or even family). All these considerations are fully applicable to disciplinary sanctions, even, given their nature, with more reason than other administrative sanctions whose disclosure may have less interference.

Therefore, it would not be justified to exclude from the scope of protection of Article 23 LTC infringements and disciplinary sanctions. And the different wording with article 21.1.b) of the LTC is not an obstacle to reaching this conclusion, which provides that access to public information may be denied or restricted if knowing it could harm the investigation or the

sanction of criminal, administrative or disciplinary offences, unlike article 23 of the LTC which only refers to the denial of access when it contains information relating to administrative offences, among other categories of data.

It should be borne in mind that both precepts give the possibility of limiting access to public information, but on the basis of two different perspectives. Thus, while article 21.1.b) of the LTC aims to limit access in order not to prejudice an investigation of a possible infringement or the execution of a penalty, to guarantee the procedure itself, the article 23 of the LTC limits access on the basis of the data protection right of the affected person.

Beyond that, although the lack of precision in this aspect of Article 23 is evident, the explanation lies not in the fact that it was intended to be distinguished from Article 21.1.b), but in the fact that the wording of article 23 obeyed precisely the reproduction of article 7.5 of the LOPD, with respect to which this Authority has systematically considered that it also includes disciplinary offenses (reports CNS 45/2015, CNS 14/2018, IAI 47/2017, IAI 30/2021 or IAI 69/2021, among others).

And not only this Authority, but also the bodies guaranteeing the right of access to public information have been interpreting it in this sense. Examples include the resolutions of the GAIP issued in claim procedures 16/2016, 249/2018, 755/2020, 47/2021, 331/2021 or 613/2021, among others, which had been interpreted in the same sense as this Authority or the resolutions of the Consejo de Transparencia y Buen Gobierno 0731-2020, 0078-2021, 0942-2020 or R.0498-2020, among others.

On the other hand, currently the provisions relating to the processing of data relating to infringements and administrative sanctions are found in article 27 of the LOPDGDD, as the LOPD has been repealed in accordance with the terms of the single repealing provision of the LOPDGDD.

Article 27.1 of the LOPDGDD provides, in relation to article 86 of the RGPD (treatment and public access to official documents), that the processing of data relating to infringements and administrative sanctions requires that the person responsible is the competent body for the instruction of the sanctioning procedure, for the declaration of infringements or the imposition of sanctions, and that the treatment is limited to the data strictly necessary for the purpose pursued by it.

It is clear that the citizen who exercises the right of access to public information is not a competent person in the sense of article 27.1 of the LOPDGDD. In these cases, the second section of this article provides that the treatment must have the consent of the person affected or be authorized by a rule with the rank of law, which must regulate the additional guarantees for the rights and freedoms of affected In other words, this section foresees two cases that enable the treatment:

a) The consent of the affected person, or
b) That the treatment is authorized by a rule with the rank of law, which also regulates additional guarantees for the rights and freedoms of those affected.

In conclusion, regardless of whether article 23 of the LTC does not contain an express reference to infractions and disciplinary sanctions, from the data protection regulations it

cannot be considered that they are excluded from the reference to infractions and sanctions administrative included in this article. "

Therefore, on the basis of what has been set forth, access to the information relating to the alleged offenders or the offenders contained in the actions and files for which access is requested must be denied, except for cases in which the commission of the offense has led to a public reprimand to the offending person, the consent of the affected person is recorded or this information is publicly available.

However, it is necessary to take into account the provision of article 25.1 of the LTC, according to which *"If any of the limits of access to public information established by the previous articles are applicable, the denial of access only affects the corresponding part of the documentation and restricted access to the rest of the data must be authorized".*

In addition, from the information available, the person making the claim seems to be in agreement with the fact that the files in question are provided anonymously .

To this end, it should be borne in mind that article 70.6.a of the RLTC defines anonymization as follows:

"[...] the elimination of the personal data of the natural persons affected contained in the information and any other information that may allow them to be identified directly or indirectly without disproportionate efforts, without prejudice to being able to maintain, where appropriate, the merely identifying data of the positions or personnel at the service of the public administrations that dictate or intervene in the administrative act."

Thus, the effect of anonymizing the file must be done taking into account that, in order for it to be considered sufficient, in terms of data protection legislation, it is necessary to guarantee that the information provided cannot relate- with an identified or identifiable natural person. In this sense, anonymization would require the elimination of all information that could allow the identification of the person or persons affected, taking into account not only the information contained in the documents that make it up but the data that can be obtained by other means, objectively assessing whether or not there is a real risk of re-identifying the affected persons without making disproportionate efforts.

Point out, with attention to the context in which we find ourselves in which files relating to the local police are requested, that the data relating to the professional identification number (TIP) constitutes for all purposes personal data, given that it also allows the identification of the person, even though, for a third party, it may require a greater effort to identify them by their TIP than by their first and last names.

In the case at hand, it must be borne in mind that the City Council has not provided any information in relation to the number of files affected, nor the people affected by the claim. This issue may be relevant for the purposes of assessing whether anonymization is an effective measure in accordance with the terms we have referred to.

For this reason, in the event that anonymization is not effective, once an objective assessment is made as to whether or not there is a real risk of re-identifying the affected persons without making disproportionate efforts, the requested information could be provided by analogously applying the solution provided for in 'article 68.4 of the RLTC, that is, *"[...] In the event that the*

content of the report may reveal information affected by the limit, the need to publish the report is understood to be satisfied with the publication of an extract or summary of the content in such a way as not to reveal the information affected by the limit."

Therefore, if the anonymization was not effective, from the perspective of data protection regulations, the person making the claim can be provided with a summary of the actions carried out, ensuring that this summary does not contain the data affected by the limit of the article 23 of the LTC or any other information which, alone or in connection with other information that can be accessed, the person making the claim may end up identifying the affected persons.

conclusion

The data protection regulations do not prevent the claimant's access to information relating to public employees who had intervened in the various previous investigation actions and disciplinary files processed between the years 2020 and 2022, both included, already resolved, that they have not participated in irregular conduct, unless there is some exceptional circumstance.

However, according to the grounds that have been set out, access to the files can be facilitated through the mechanism of anonymization or, when this measure is not effective, through a summary of the files, of in such a way that in no case are the physical persons affected identifiable (persons under investigation and, where appropriate, whistleblowers or witnesses).

Barcelona, July 6, 2023