IAI 6/2022

Supplementary report issued at the request of the Commission for the Guarantee of the Right of Access to Public Information in relation to the request for a report that a Department of the Generalitat would have made to the GAIP, in the framework of the mediation session of the Claim (...).

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, in relation to the request for a report that the regional administration would have made to the GAIP, as part of the mediation session of the Claim (...).

In the mediation agreement of January 27, 2022, regarding the claim (...), the claimant and the Department would have agreed to request a report from the GAIP "on whether it is legally feasible to make a copy of a month of registration and which data in the copy is appropriate for a person who has the status of a journalist to access.

Given this request for an opinion from the GAIP, agreed in the mediation agreement, the GAIP asks the Authority to issue a report in relation to access to the data of the Access Register of the Palace of the Generalitat, having considering that said Register contains personal data. The GAIP requests the opinion of the Authority in order to be able to take it into account in the legal evaluation of the opinion that will be issued by the Commission itself.

Having analyzed the request, which is accompanied by a copy of the minutes of the mediation session, and the documentation of the corresponding file, and in accordance with the report of the Legal Counsel, issue the following report:

Background

1. On August 23, 2021, a citizen submitted a letter to the Department, in which he requested to know the access control to the Palau de la Generalitat, specifically:

> **"(...). The details of each and every person who has accessed the Palau de la Generalitat from January 1, 2021 to the present day. I request that for each one of them be indicated: the number and details of the employment of the person making the visit, the date of the visit, the number and position of the person visited in the complex and the time of entry and the exit to the complex. (...)."**

2. On November 5, 2021, the applicant filed a complaint with the GAIP, given that, as he explains, he would not have received the requested information. According to the claimant, "The Presidency claims that it does not keep the data for that long and that it only has them for the last month. In that case, you should apply partial access and deliver at least that last month."

3. On November 29, 2021, the GAIP requested 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 governance, in relation to the Claim.

4. On January 12, 2022, the Authority sent the GAIP the IAI Report 83/2021, which concludes the following:

> **"The data protection regulations do not prevent access to information relating to visits by people belonging to interest groups, nor to information on visits directly related to the public activity of the Administration (protocol visits, institutional meetings, etc).**
>
> **Information about visits by people who act on behalf and representation of legal entities, for purposes other than those of interest groups, can be provided by omitting the identity of the specific person who represents them, unless consent is obtained expressed by the people affected or it is data made manifestly public by these people.**
>
> **The data protection regulations would not enable the general communication of the identity of third-party natural persons who act on their own behalf and who visit the Department's premises.**
>
> **Without prejudice to the obligation of transparency regarding the public agendas of senior positions or managerial staff and staff assimilated to general sub-directorate, it also does not seem justified to facilitate generalized access to the identity of each and every public worker who receives visits."**

5. The file contains a copy of the Minutes of January 26, 2022, of the mediation session relating to the Claim, as well as a copy of the Mediation Agreement, dated January 27, 2022, in which the parties agree to formally ask the GAIP to issue a legal opinion through an Opinion "on whether it is legally feasible to make a copy of a month's registration and on which data in the copy is appropriate for a person who has the condition of a journalist."

6. On the same date of January 26, 2022, the Department sends a letter to the GAIP in which it requests a report on "whether it is appropriate to block the data in the event that a request for access to the public information."

7. On February 14, 2022, the Department will send, at the request of the GAIP, the formal request for an opinion in relation to the following aspects:

> **"Legal feasibility or not of blocking the data of a data processing subject to automatic deletion in application of the provisions of Instruction 1/1996 of the Spanish Data Protection Agency based on a request for access to information public, bearing in mind that, in accordance with the regulations, the information is destroyed automatically within one month of its collection.**

At this point, the report of the GAIP is requested, without prejudice to the fact that the specific controversy about the basis for blocking this data, the destruction of which derives from Instruction 1/1996, we understand that it is appropriate to determine it in the 'Catalan Data Protection Authority (APDCAT).

In the case of ruling on the feasibility of blocking, establish which data from those available in the treatment can be provided, taking into account the purpose of the data collection, and the considerations made in the report issued by the APDCAT. "

8. On February 22, 2022, the GAIP requests this Authority to issue a report on the issue raised, in order to be able to take it into account in the legal assessment of the opinion that the GAIP will 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 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.

In the case at hand, the APDCAT issued report IAI 83/2021, in relation to the Claim (...), and issues a complementary report, at the request of the GAIP, on the issues raised by the Department in Claim mediation procedure, mentioned.

This report is issued exclusively with regard to the assessment of the impact that the requested access may have on the personal information of the persons affected (Article 4.1 of 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 (hereafter, RGPD).

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 Claim (...), in relation to which this supplementary report is issued, is filed against the denial of access to information relating to the register of people who would have accessed

at the Palau de la Generalitat from January 1, 2021 until the moment of formulating the request (August 23, 2021), specifically, "the number and details of the employment of the person who performs the visit, the date of the visit, the number and position of the person visited in the complex and the time of entry and exit to the complex."

As this Authority has done in accordance with report IAI 83/2021, issued at the request of the GAIP in relation to the Claim (...), the data of the natural persons who have accessed the Palau de la Generalitat during the period in which the request refers to, as well as the data of the people receiving the visit, are personal data and are protected by the principles and guarantees of the data protection regulations.

Without prejudice to the considerations made in the IAI Report 83/2021, to which we refer, in this report it is necessary to analyze the issue raised by the Department at the GAIP, on which the GAIP requests the opinion of this Authority, specifically:

> **"Legal feasibility or not of blocking the data of a data processing subject to automatic deletion in application of the provisions of Instruction 1/1996 of the Spanish Data Protection Agency based on a request for access to information public, bearing in mind that, in accordance with the regulations, the information is destroyed automatically within one month of its collection.**
>
> **At this point, the report of the GAIP is requested, without prejudice to the fact that the specific controversy about the basis for blocking this data, the destruction of which derives from Instruction 1/1996, we understand that it is appropriate to determine it in the 'Catalan Data Protection Authority (APDCAT).**
>
> **(...)"**

Given the subject of the report in these terms, it is necessary to start from the basis that any processing of personal data must comply with the principles and guarantees established in the regulations (RGPD).

According to article 5.1 RGPD: "The personal data will be: (...).

> **b) collected for specific, explicit and legitimate purposes, and will not be subsequently treated in a manner incompatible with said purposes; in accordance with article 89, section 1, the further processing of personal data for archival purposes in the public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes ("limitation of the purpose") ;" (...).**
> **e) maintained in a way that allows the identification of the interested parties for no longer than necessary for the purposes of the treatment of personal data; personal data may be kept for longer periods as long as they are treated exclusively for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89, section 1, without prejudice to the application of the measures appropriate technical and organizational techniques that this Regulation imposes in order to protect the rights and freedoms of the interested party ("limitation of the conservation period");**

(…).”

The person in charge must apply the principle of limitation of the retention period, taking into account the purpose that a certain treatment of personal data may have, in order to ensure that the treatment does not extend beyond what is necessary to achieve the purpose (art. 4.7 and art. 5.2 RGPD). This, without prejudice to the conservation, if applicable, for the ulterior purposes that are compatible under the terms of the data protection regulations.

Therefore, at the outset, it is clear that the retention of personal data will depend in each case on what is necessary to fulfill the purpose of the treatment.

Within the framework of the aforementioned principles of limitation of the retention period and limitation of the purpose, article 32 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), imposes on the data controller - in the case in question, the Department - the obligation to block the data:

"1. The person responsible for the treatment will be obliged to block the data when it proceeds to its rectification or deletion.

2. The data blocking consists in the identification and reservation of the same, adopting technical and organizational measures, to prevent its treatment, including its display, except for making the data available to judges and courts, the Ministry of Finance or the competent Public Administrations, in particular the data protection authorities, to the requirement of possible responsibilities derived from the treatment and only for the prescription period of the same.

After that period, the data must be destroyed.

3. Blocked data may not be processed for any purpose other than that indicated in the previous section.

(...)”.

Therefore, blocking is an obligation that the person in charge must necessarily apply, and only with the exceptions provided for by law, when the rectification or deletion of data must be carried out.

Based on this general obligation to block the information that must be deleted (according to the term established for each treatment), it must be understood that the deletion is not equivalent, at the outset, to the physical destruction of the information.

It is worth noting that the blocking obligation, provided for in the LOPDGDD in general, admits some exceptions that the same rule makes explicit (such as, in relation to treatments for the purpose of video surveillance, ex. art. 22.3 LOPDGDD, or in relation to data processing in internal complaints information systems, eg art. 24.4 LOPDGDD). In these cases, the rule makes it clear that the blocking of the information does not apply, therefore, the physical destruction of the information can proceed, once the retention period has been fulfilled.

However, beyond these exceptions, it must be understood that the blocking obligation operates whenever personal information must be deleted. Therefore, in principle, also in relation to the case at hand (deletion of data from the Department's access control).

As stated in the IAI Report 83/2021, according to the Department's report of November 29, 2021 (issued at the request of the GAIP in relation to the Claim ...), the information requested by the claimant would be part of the "Presence Control" treatment, included in the Department's Treatment Activity Register (RAT).

As can be seen from the available information (Mediation Act of January 26, 2022), the Department would have expressed doubts "about whether the request for access to public information itself enables the procedure to suppress the automatic destruction of the data, given that they must block a deletion of an automated procedure, that is to say, that data that should have been deleted must be blocked" (reason for which this Authority is requested to be consulted) .

As can also be seen from the available information (Mediation Act of January 26, 2022, and request for Opinion to the GAIP, of February 14, 2022), the Department considers that the retention period provided for the treatment of data of the "Presence Control", is for one month, and that the obligation to effectively destroy the data in this period of one month derives from "Instrucción 1/1996, of March 1, of the Agency of Data Protection, on automated files established for the purpose of controlling access to the buildings", which is attached to the file.

Thus, the Department bases the obligation to delete (destroy) access control data within one month, in the provisions of rule 5 of Instruction 1/1996, which provides that "Personal data must be destroyed when the period of one month has passed, counted from the moment they were collected."

However, it should be pointed out at the outset that the establishment of the retention period for the information in the case at hand is the responsibility of the person in charge, that is, the Department itself.

This obligation of effective destruction within one month does not seem to be based on a rule (Instruction 1/1996 of the AEPD) that is issued on the basis of a regulation (Organic Law 5/1992) previously to the regulations in force on data protection, and of lower rank than the LOPDGDD. But in addition, this Instruction issued by the Spanish Data Protection Agency does not apply to entities that, in accordance with article 156 of the EAC, are part of the scope of action of the 'APDCAT, as is the case of the claimed Department.

Beyond this, it is also necessary to take into account what is established in the Department's record of processing activities.

Article 30.1 of the RGPD indicates the information that the RAT must contain, among others: "f) when possible, the deadlines for the deletion of the different categories of data; (...)."

The Department's RAT foresees, for the "Presence Control" treatment, conservation for a period of "less than one year". Therefore, at the outset, and according to the manager's own RAT, it does not seem that the retention period must necessarily be one month.

In addition, the Document Access and Assessment Table -TAAD- (Code 869 of the Documentary Series "Register of access of external persons to administrative offices"), applicable to the "control of people's access to the centers of work and administrative dependencies", which provides for total destruction, and a term (which should be understood as a maximum) of four years.

At this point reference should be made to Law 10/2001, of 13 July, on archives and documents, which aims to "promote the management and guarantee the preservation of documentation in Catalonia, both public and private, in accordance with its values, to put it at the service of general interests; to establish the rights and duties of those who hold them, and also of citizens in relation to the aforementioned documentation, and to regulate the Catalan Archives System." (art. 1 Law 10/2001).

According to article 2 of Law 10/2001, for the purposes of this Law it is understood by:

> **"(...).**
>
> **h) Documentation in active phase: the administrative documentation that a unit processes or routinely uses in its activities. Legal Portal of Catalonia**
>
> **i) Documentation in semi-active phase: the administrative documentation that, once the ordinary processing is concluded, is not used in a usual way by the unit that produced it in its activity.**
>
> **j) Inactive or historical documentation: administrative documentation that, once the immediate administrative validity has ended, has values primarily of a cultural or informative nature."**

For the purposes concerned, the documentation generated by data processing for the purpose of controlling visits and access to public buildings, would be in an active or semi-active phase, while the Department, as responsible, must routinely use that information, or must have it on time.

Specifically, taking into account what the Department itself (RAT) would have determined, it seems that the access control documentation could be in an active or semi-active phase for a maximum period of one year. In any case, and given that the RAT specifies a term of conservation for a period of "less than a year", the period could be less than a year, if so established by the Department.

Once the active or semi-active phase has concluded (a period which, as we have said, would correspond to the maximum period of one year set by the Department), and taking into account the provisions of the aforementioned TAAD, the person in charge should also maintain the information , until completing the maximum term of four years provided for by the TAAD.

Thus, even though, after the maximum period of one year set by the Department, the access control information should no longer be processed, it should still be kept until the aforementioned 4-year period is completed. It is in this period (once the period of a maximum of one year has passed, until the 4-year period provided for in the TAAD to be able to destroy the documentation is completed), that the blocking of personal data would operate, in the terms of article

Blocking the data would allow the person in charge to have the information, only if it was necessary to process it to deal with possible responsibilities.

In any case, it is clear from all the above that the Department would not be "obliged" to destroy access control information by application of Instruction 1/1996, as has been said, nor would this effective destruction of information 'must do within a month. On the contrary, the information can be treated until completing the maximum term of one year, and should be kept properly blocked, until completing the term of 4 years, mentioned.

III

Article 32 of the LOPDGDD defines the blocking duty:

> **"1. The person responsible for the treatment will be obliged to block the data when it proceeds to its rectification or deletion.**
> **2. The blocking of the data consists in the identification and reservation of the same, adopting technical and organizational measures, to prevent its treatment, including its visualization, except for the provision of the data to judges and courts, the Ministry of Finance or the competent Public Administrations, in particular the data protection authorities, for the requirement of possible responsibilities derived from the treatment and only for the prescription period thereof.**
> **After that period, the data must be destroyed.**
> **3. Blocked data may not be processed for any purpose other than that indicated in the previous section. (...)"**

So, once the block has been applied, article 32.2 of the LOPDGDD limits the processing of the blocked data to certain cases: making the data available to judges and courts, the Public Prosecutor's Office or the competent public administrations, in particular from the data protection authorities, for the requirement of possible responsibilities arising from the treatment until they have prescribed.

This regulatory provision is certainly restrictive in relation to the cases in which the blocked information can be the subject of treatment.

Now, beyond the literalness of article 32.2 LOPDGDD, which establishes a closed list regarding the possible recipients of blocked personal information and specifies the purpose of blocking in the demand for responsibilities derived from the treatment, it does not seem possible deny access to blocked data, for example, by an affected person exercising the right of access to their own personal information (art. 15 RGPD).

As this Authority has decided (report CNS 76/2016), it may be lawful for a controller to process certain blocked personal data, in order to fulfill a certain legal obligation, for example, to allow the exercise of a right by a certain person. This has also been recognized by the Spanish Data Protection Agency in several resolutions related to this matter (among others, Resolutions 00665/2021, 00532/2020, or 00484/2021).

Although in the case at hand it is not the holder of the personal information who requests access to the Department's visit control in exercise of the right of access provided for in Article 15 RGPD, but a third party, in accordance with what has been set out, the blocking of personal information should also not void the possibility of exercising other rights, such as the right of access to public information, under the terms of transparency legislation. Especially if, as in the case we are dealing with, the data has been blocked at a time prior to the deadline that derives from the record of processing activities of the person in charge.

When this right is exercised, obviously the requested Administration cannot be required to provide information that it does not have. As was already agreed in Report IAI 83/2021, in the case we are dealing with, the Department does not have to provide, in fact it cannot, even if it wants to, the access control information it has already removed.

However, the information that is blocked, although it is subject to a strict access regime (art. 32 LOPDGDD), has not yet been eliminated.

The purpose of communicating blocked data would be to comply with an obligation of the responsible entity, based on the Constitution (art. 105.b) CE) and the LTC. This attention to the Department's responsibilities in this matter seems to have a place in the purposes for which article 32 LOPDGDD provides that blocked data can be used.

Thus, access to certain personal information blocked by the Department's access control (in the terms already set out in the IAI report 83/2021), could be justified and enabled by the exercise of the right of access to public information by a citizen, on the one hand, and by the obligation of the person in charge to attend to this right, on the other, with respect to the public information he has in his possession.

From the perspective of data protection regulations, the processing, specifically, the communication of certain access control data to a citizen who exercises the right of access to public information, would be enabled by article 6.1. c) of the RGPD, according to which the treatment is lawful if it is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment - in this case to comply with the transparency legislation -, without the blocking of the information may prevent the exercise of this right.

For everything that has been explained, the blocking of information from the Register of visits to the Palau de la Generalitat (access control), which the Department would have, is considered feasible and adjusted to the data protection regulations, in the terms set forth in this report.

IV

Given the affirmative answer to the first question raised about the legal viability of the block in the case examined, it is necessary to refer to the following question raised by the Department sent to the GAIP and which it forwards to the Authority:

> **"In the case of ruling on the feasibility of the blocking, establish which of the data available in the treatment can be provided, taking into account the purpose of the collection of the data, and the considerations made in the report issued by the APDCAT ."**

At the outset, as stated in Legal Basis III of Report IAI 83/2021, as stated in the corresponding file, the claimant requested to know "the number and details of the employment of the person making the visit, the date of the visit, the number and position of the person visited in the complex and the time of entry and exit from the complex (...)."

As stated in point three of the Mediation Agreement of January 27, 2022, "The parties recognize the right of the person claiming to formally request the same information on the Registry (...), but of a different temporal scope (...)."

Bearing this in mind, we note that this Authority already ruled on access to the requested data, in Report IAI 83/2021. For the purposes of interest, it should be remembered that access to the requested public information must have a different response in different cases analyzed and depending on the groups or natural persons affected (interest groups, natural persons representing of legal entities, natural persons acting in their own name, etc.), in application of the own transparency legislation and data protection regulations.

In this sense, we refer to the considerations of FFJJ IV to VI of Report IAI 83/2021, as well as to the conclusions of said report:

> **"The data protection regulations do not prevent access to information relating to visits by people belonging to interest groups, nor to information on visits directly related to the public activity of the Administration (protocol visits, institutional meetings, etc).**
>
> **Information about visits by people who act on behalf and representation of legal entities, for purposes other than those of interest groups, can be provided by omitting the identity of the specific person who represents them, unless consent is obtained expressed by the people affected or it is data made manifestly public by these people.**
>
> **The data protection regulations would not enable the general communication of the identity of third-party natural persons who act on their own behalf and who visit the Department's premises.**
>
> **Without prejudice to the obligation of transparency regarding the public agendas of senior positions or managerial staff and staff assimilated to general sub-directorate, it also does not seem jus**

facilitate generalized access to the identity of each and every public worker who receives visits."

Beyond reiterating these conclusions, which answer the question posed, we note that, according to the Minutes of the mediation session of January 26, 2022, the representatives of the Department insisted that: "the specific purpose is to know who is there and does not indicate which person is entering and who is going to see." According to the Act itself, the Department insists that "the control of the register is done exclusively for security reasons and to know who is in the Department and it may not be possible to know who is going to see."

Regarding this, it should be noted that the file sent to this Authority contains a copy of the "Visit Control List", which includes the fields that the Department would collect in the access control. According to this list provided by the Department itself, the fields are the following:

"Visit: State Start date. End Date Headquarters/Delegation Observations visit. Visitor: Name. Surnames. IDENTITY CARD. Visiting company Employee: Name Employee. Surname Employee Department."

It seems clear, therefore, that the Department would have information about the person making the visit, and about the person visited. This, without prejudice to the fact that the purpose of the treatment is a security purpose which, as already stated in Report IAI 83/2021 (FJ II), is also not relevant when determining what is public information for the purposes of article 2.b) LTC.

In any case, given the information fields that, due to the available information, the visit control list includes, the information can be provided in response to the considerations already made in said report.

Thus, for example, in the event that the Department has information on natural persons acting on behalf and representation of legal persons, as is done in FJ VI of Report IAI 83/2021, in certain cases it will be relevant omit the identity of these natural persons, and indicate only "the visiting company".

Likewise, by application of the principle of minimization, according to which the data processed must be adequate, relevant and limited to what is necessary in relation to the purposes of the treatment (art. 5.1.c) RGPD), we agree that no it would be appropriate to communicate the ID of the people who visit the Department, which is included in the aforementioned Visit Control List.

Finally, regarding the "Visit comments" field, it seems that it could refer to the reason for the visit.

On this, in summary, and without prejudice to refer to the considerations of the IAI Report 83/2021, it can be noted that, except for visits by people belonging to interest groups or visits directly related to the activity public of the Administration (protocol visits, institutional meetings...) or that referred to representatives of legal entities, it does not appear that the data protection regulations enable this type of information to be provided on the reasons for the visit, in a generalized way.

For all this, the following conclusions are made,

conclusion

From the perspective of data protection regulations, it is viable to keep the information from the Department's access register properly blocked, based on the general blocking obligation of article 32 of the LOPDGDD once the phase is active or semi-active has concluded (within the maximum period of one year set by the RAT). The Department should keep the information blocked, until completing the maximum term of four years provided for b

Access to blocked public information must have a different response depending on the groups or natural persons affected (interest groups, natural persons representing legal entities, natural persons acting on their own behalf, etc.), in application of transparency legislation and data protection regulations. We refer to this in the legal foundations IV to VI and the conclusions of the IAI Report 83/2021 of this Authority.

Barcelona, March 24, 2022