

Ref.: IAI 42/2018

## **Claim: 269/2018**

### **Legal report issued at the request of the Commission for the Guarantee of the Right of Access to Information Public in relation to the claim for the denial of access to a list of different data broken down for each educational center in Catalonia**

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 claim 269/2018 presented in relation to the denial of access to list of different data broken down for each educational center in Catalonia.

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 May 29, 2018, a citizen submitted a request for access to public information, in accordance with Law 19/2014, of December 29, on transparency, access to public information and good governance , to the Department of Education of the Generalitat of Catalonia, in which he asks:

" The list of broken down data for each educational center in Catalonia that included: a) Number of students b) Number of units c) Type of center (by courses taught) d) Ownership (public, private or chartered) e) Educational area f) Number of foreign students g) Number of students with special educational needs due to unfavorable social situation h) Number of students who receive individual dining allowances i) Number of students enrolled outside the enrollment period j) Demand received during pre-registration k) Premature school dropout rate l) Family income (grouped by income levels)

In case of incurring any of the limitations of the right of access to public information, I request a list of the anonymized data (for example, using a code instead of the name of the center that is the same for all the data requested ).

But in any case, a report of the individual data of each center, in no case grouped.

I request the absolute number of the data and, only if this is not possible, the percentage of the total number of students in the case of the data requested in sections (f), (g), (h) and (i) .”

2. On June 29, 2018, the General Secretary of the Department of Education issues a resolution approving the request for access to the information presented and agreeing to provide the information in the terms indicated in the same resolution.

3. On July 20, 2018, the person requesting access to the information submitted to the GAIP a claim against the Department of Education, considering that he had not been provided with all the information requested. Specifically, he argues that:

- "- The information on foreign students or students with special educational needs has not been given by educational center but grouped by municipality (points f) ig) of the SAIP)
- Only the information of students enrolled outside the enrollment period of the first year of each educational stage was given when information was requested for all courses (point i) of the SAIP)
- Academic courses are not specified in the publication on the website Open data regarding students and units (points a) and b) of the SAIP)."

4. On August 1, 2018, the GAIP transfers the claim submitted to the Department of Education and requests the corresponding report as well as the completed file.

5. On September 18, 2018, the Department of Education issues a position report on the claim presented in which it states, with regard to the data protection limit, that:

"(...)the Department considers that information about foreign students and students with special educational needs should be denied at the educational center level, taking into account that racial origin and health are personal data specially protected from in accordance with art. 23 of Law 19/2014, of December 29, on transparency, access to public information and good governance.(...)"

6. On September 20, 2018, the GAIP requests this Authority to issue a report 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 under the terms of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data (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

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

Article 18 of the LTC establishes that "people have the right to access public information, referred to in article 2.b, in an individual capacity or in the name and representation of any legally constituted legal person" (section 1). The mentioned article 2.b) 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 the which are supplied by the other obliged subjects in accordance with the provisions of this law".

Law 19/2013, of December 9, on transparency, access to public information and good governance (LT) is pronounced in similar terms in its articles 12 (right of access to public information) and 13 (public information).

However, in accordance with article 20 and s. of the LTC, the right of access to public information may be denied or restricted for the reasons expressly established in the laws. Specifically and with regard to information that contains personal data, access must be denied if the information to be obtained contains particularly protected data, unless there is express consent from the interested parties (art. 23 LTC).

In the event that the information to which you want to access does not contain specially protected data, to determine the extent of the limit it is necessary to balance the right to data protection of the affected persons, and the public interest in disclosure of the information (art. 24 LTC).

### III

In the application for access presented to the Department of Education, and for the purposes of this report, it is requested to access the number of foreign students and the number of students with special educational needs due to unfavorable social situation in all centers educational institutions of Catalonia.

In order to determine whether this request for information is subject to the limits regulated in articles 23 and 24 of the LTC it is necessary to analyze whether the information requested contains personal data and whether the regime is therefore applicable provided for in the RGPD.

The RGPD applies to the fully automated processing of personal data, as well as to the non-automated processing of personal data contained in a file or intended to be registered in it (Article 2.1).

For the purposes of the RGPD, all information about an identified or identifiable natural person (the interested party) is considered "personal data"; in accordance with the second section of article 4.1 of the RGPD "an identifiable natural person shall be considered any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of the physical, physiological, genetic, psychological, economic, cultural or social identity of this person" (article 4.1 RGPD).

In this sense recital 26 of the RGPD states that: "The principles of data protection apply to all information relating to an identified or identifiable natural person (...)

To determine whether a person is identifiable, it is necessary to take into account all the means that the controller or any other person can reasonably use to directly or indirectly identify the natural person, such as singulation. In determining whether there is a reasonable likelihood that means will be used to identify a natural person, all objective factors, such as the costs and time required for identification, must be considered, taking into account both the technology available at the time of the treatment as technological advances."

Article 4.5 of the RGPD defines pseudonymization as "the processing of personal data in such a way that they can no longer be attributed to an interested party without using additional information, provided that this information is recorded separately and is subject to technical and organizational measures aimed at guaranteeing that the personal data are not attributed to an identified or identifiable natural person". In such a way that recital 26 of the RGPD makes it clear that "pseudonymized personal data, which could be attributed to a natural person using additional information, must be considered information about an identifiable natural person".

Therefore, personal data is any information relating to a natural, living, identified or identifiable person. The various information collected that can lead to the identification of a certain person also constitute personal data. Thus, a natural person is not considered identifiable if the identification requires disproportionate time frames or activities taking into account the costs, the time required for the identification and the available technology.

On the contrary, Recital 26 of the RGPD states that "(...)the principles of data protection do not apply to anonymous information, that is to say to information that is not related to an identified natural person or identifiable, nor to the data converted to anonymity in such a way that the interested party is not identifiable or ceases to be so. Consequently, this Regulation does not affect the treatment of this anonymous information, even for statistical or research purposes."

It must be taken into consideration that for the data to be considered truly anonymous, the anonymization must be irreversible. Personal data that has been anonymised, encrypted or presented under a pseudonym, but that can allow a person to be re-identified, remains personal data and is included in the scope of the GDPR. The decision on whether the data allows the identification of a person and on whether the information can be considered anonymous or not, depends on the specific circumstances of each case and is included in the risk analysis that the data controller must be carried out prior to the processing of the data.

In this sense, the conclusions of the Working Group of article 29 in the Opinion 4/2007 "on the concept of personal data", which analyzes the definition of personal data provided for in article 2 a) of Directive 95/46/EC, and which determines:

"For the purposes of the Directive, "anonymous data" can be defined as any information relating to a natural person that does not allow identification by the person responsible for the treatment of the data or by any other person, taking into account the set of means that can reasonably be used by the person responsible for the treatment or by any other person, to identify said person. "Anonymized data" will therefore be anonymous data that previously referred to an identifiable person, whose identification is no longer possible. Recital 26 also refers to this concept when it says that "the principles of protection will not apply to those data made anonymous in such a way that it is no longer possible to identify the interested party". Once again, the decision on whether the data allows the identification of a person and on whether the information can be considered anonymous or not depends on the specific circumstances of each case, so a case-by-case analysis must be carried out, in which special attention must be paid to the extent to which it is reasonably possible to use the means to identify that person, as described in recital 26. This is particularly important in the case of statistical information, since despite that this can be provided in the form of aggregated data, the original sample may not be sufficiently wide and other data may allow the identification of physical persons.

---

---

---

It is also necessary to take into consideration the Opinion 05/2014 on anonymization techniques, of the Article 29 Working Group, which formulates recommendations for the management of the techniques

of anonymization taking into account the residual risk of identification inherent in the same. In this opinion it is made clear that the concept of identification does not only involve the possibility of recovering the name or address of a person, but also includes "potential identifiability through singularity, linkage or inference", that is to say, it is not only about the possibility of direct identification of the person, but also indirect.

Therefore, the Department of Education, as responsible for the treatment, in the process of anonymizing the data must assess the risks and the possibility of subsequent re-identification of the data holders taking into account the concerted circumstances of each case i, must guarantee the confidentiality of the personal information it has anonymized.

It must be taken into consideration that the holders of the data that have been anonymized by the Department of Education are minors, and that as such, by application of the legal principle of the best interests of the minor, they deserve special protection.

In the case we are concerned with, the information requested by the claimant, consisting of the number of foreign students and the number of students with special educational needs due to the unfavorable social situation of educational centers in Catalonia, is information that does not contain, in principle, personal data.

Knowing the number of foreign students enrolled in a center, the number of students with special educational needs due to unfavorable social situation, individualized by center, the number of students who receive dining allowances, the number who have been schooled outside the period of enrollment or the dropout rate, does not allow directly identifying the students affected. Nor should it escape us, that in certain circumstances it can be relatively easy for some of this information to be known by other students at the center (for example, the status of a foreigner, schooling outside the enrollment period, or the existence of special educational needs). In this case the knowledge of these circumstances would not derive from the information that is now being requested but can be easily obtained directly by other means.

However, in centers with a small number of students in which the different characteristics for which information is requested, if, in addition to the information relating to the number of foreigners in the center, other information such as the number of students with special educational needs due to an unfavorable family situation, or the number of students who receive individual dining allowances, it may end up being relatively easy to obtain a profile of certain students that is easily identifiable not only by the rest of the families from the center but by many other people. For this reason, in these specific cases the Department would need to facilitate the information at a level of aggregation that would guarantee the non-identification of the interested parties. And in this case, the level of aggregation might not be sufficient at the municipal level, because surely many of the cases in which there is a risk of re-identification at the center level, the same risk would also exist at the municipal level when it comes to municipalities with a single center

In the rest of the cases, the regulations on the protection of personal data would not prevent access by the claimant to the requested information to the extent that no personal data or information that indirectly allows the identification of the data holders is provided.

Article 25 of the LTC provides that in cases where any of the limits on access to public information provided for in that rule are applicable, the denial must only affect the corresponding part of the documentation that is affected for that limit while access to the rest of the unaffected data must be authorized. Therefore, nothing would prevent the information from being delivered at the center level when there is no risk of re-identification, and from providing it at the municipality level or even at a higher level (for example, rural school zone) when this circumstance does not occur.

It does not escape our notice, however, that providing information on the number of foreign students by level and by center throughout Catalonia involves providing information that can lead to drawing up a profile of these centers based on the nationality of their students and which, as a consequence, could have a stigmatizing effect on centers that concentrate a greater number of "foreign" students, but, in any case, this issue would escape the scope of the protection of personal data.

### **conclusion**

The regulations on the protection of personal data do not prevent the claimant from accessing information on the number of foreign students and the number of students with special educational needs due to unfavorable social conditions in all educational centers in Catalonia.

In those cases in which, based on a risk analysis and in a motivated way, there is a risk of identification of the data holders, the information can only be delivered at a level of aggregation that guarantees non-identification.

Barcelona, 9 October 2018