CNS 7/2019

Opinion in relation to the query formulated by an AFA of a public school regarding the adaptation of its actions to the data protection regulations.

A letter from an AFA of a public school is presented to the Catalan Data Protection Authority, in which a query is formulated on how to adapt its actions to the data protection regulations.

The consultation is accompanied by a document called "Data protection impact assessment".

Having analyzed the request, and the documentation that accompanies it, and having seen the report of the Legal Counsel, the following is ruled

I

(...)

II

The AFA requests the advice of the APDCAT in order to adapt to the data protection regulations and provides with the request a document called "Impact assessment relative to the protection of data".

The AFA, in order to achieve its objectives, processes information about its members, students, collaborators, workers and volunteers. These data, to the extent that they refer to identifiable natural persons, are considered personal data and are therefore protected by the regulations on the protection of personal data.

Consequently, any treatment of this data, including the collection or any subsequent use or treatment of it, is subject to the principles and guarantees contained in the data protection regulations. Specifically, in Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereafter RGPD) and Organic Law 3/2018, of December 5, of Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD).

Having said that, and with regard to the document called "data protection impact assessment" that is attached to the consultation, the data protection regulations provide that prior to the start of the treatment, the responsible must make an assessment of the impact on data protection (hereafter AIPD) when this treatment, due to its nature, scope, context or purposes, poses a high risk for the rights and freedoms of natural persons, especially when new technologies are used (recital 76 and article 35 of the RGPD).

Thus, on the one hand, article 35.3 of the RGPD establishes that, among other cases, an impact assessment relating to data protection must be carried out in the following cases:

a) Systematic and comprehensive evaluation of personal aspects of natural persons based on automated processing, such as profiling, on the basis of which decisions are taken that produce legal effects for natural persons or that significantly affect them similar way

b) Large-scale processing of the special categories of data referred to in Article 9, paragraph 1, or of personal data relating to convictions and criminal offenses referred to in Article 10.

c) Large-scale systematic observation of a public access area.

For the delimitation of what is to be understood by "large-scale processing", the Article 29 Group, in its opinion on the appointment of data protection delegates, considers that the following should be taken into account:

-The number of interested parties affected, either in absolute terms or as a proportion of a certain population.
-The volume and variety of processed data.
-The duration or permanence of the treatment activity.
- The geographical extent of the treatment activity.

In addition, the LOPDGDD (DA 17ª) has expressly provided that an impact assessment will need to be carried out to determine the risks derived from treatments for the purposes of public health research and, in particular, biomedical research, which will have to specifically assess the risks of re-identification linked to the anonymization or pseudonymization of the data.

On the other hand, beyond the cases provided for directly in the RGPD and the LOPDGDD, and following the Guidelines on the impact assessment related to data protection (AIPD) and to determine if the treatment probably entails a high risk for the purposes of Regulation (EU) 2016/679, adopted by the Article 29 Working Group on April 4, 2017 (hereinafter, WP 248), this Authority, in the treatments that are not cross-border, considers that it is necessary carry out an impact assessment relating to data protection in the treatments that you wish to carry out that meet two or more of the following circumstances:

- Evaluation or "scoring" of people, including the creation of profiles and the prediction of behaviors.
- Automated decision-making with significant legal or similar effect.
- Systematic observation.
- Sensitive data or very personal data (special data categories of Article 9 RGPD or personal data relating to convictions and criminal offenses referred to in Article 10 RGPD).
- Large-scale data processing.
- Association or combination of data set that may exceed the reasonable expectations of interested parties.
- Data relating to vulnerable subjects (minors, employees, disabled people, elderly people, asylum seekers or refugees, etc.).
- Innovative use or application of new technological solutions or organizational
- When the treatment prevents the affected persons from exercising a right, using a service or executing a contract.

The data protection impact assessment, in principle, should not refer to all the activities carried out by a person in charge or a person in charge of the treatment, but only to those in which the aforementioned circumstances occur.

Taking all this into account, this Authority considers that the treatments described in the AFA are not included in any of the cases currently provided for in the data protection regulations nor in the circumstances established by this Authority in which it must be carried out, in advance to its treatment, an impact assessment. Therefore, in this specific case, the AIPD would not be mandatory, although nothing prevents it from being done on a voluntary basis.

In any case, the document provided by the association and called "Data protection impact assessment" does not include the minimum content established by article 35.7 of the RGPD and, therefore, cannot be considered an AIPD. This does not mean that this Authority values the effort made by the AFA to comply with data protection regulations.

For information, you can consult the Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPA) and to determine whether the processing is likely to involve a high risk for the purposes of the Regulation (EU) 2016/679 (WP 248), adopted by the European Data Protection Committee at its meeting of May 25, 2018, and the APDCAT's Practical Guide on impact assessment related to data protection in RGPD (http://apdcat.gencat.cat/web/.content/03-documentation/).

III

Having said that, in order to comply with data protection regulations, you must comply with all the obligations set out in the General Data Protection Regulation. In this report, with the aim of giving you the necessary support so that you can adapt, we provide you with general information about some of the obligations that you must take into account when processing data. However, responsible compliance with the provisions of the Regulation requires a careful analysis of all the obligations provided for in the RGPD taking into account the specific circumstances of each of the treatments carried out.

The AFA must comply with the provisions of the RGPD. Therefore, data processing must always be carried out respecting the principles of the RGPD (art. 5 RGPD) and in such a way that compliance can be demonstrated (proactive and demonstrable responsibility).

Personal data must be treated according to the principles set out in Article 5 of the RGPD. Thus, the data must be:

a. Treated lawfully, loyally and transparently in relation to the interested party (lawfulness, loyalty and transparency). b. Collected for specific, explicit and legitimate purposes and subsequently must not be treated in a manner incompatible with these purposes. c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization). d. Accurate and, if necessary, should be updated. e. Kept in such a way as to allow identification of the interested parties for a period no longer than is necessary for the purposes of processing personal data ("retention period limitation"). f. Treated in such a way as to guarantee adequate security ("integrity and confidentiality").

In accordance with the principle of legality, the data controller can only treat them if one of the legal bases established in article 6 of the GDPR applies. Specifically:

a. That has the consent of the affected person for one or more specific purposes. b. That it is necessary to execute a contract to which the interested party is a party or for apply pre-contractual measures at the request of the interested party.

c. That it is necessary to fulfill a legal obligation of the person in charge of treatment.

d. That it is necessary to protect the vital interests of the interested party or another natural person

e. That it is necessary to fulfill a mission carried out in the public interest or in the exercise of public powers granted to the data controller. f. That it is necessary to satisfy legitimate interests pursued by the person in charge of the treatment or by a third party, provided that there are no interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a minor.

In the case of treatments necessary for the fulfillment of a legal obligation (letter c) or a mission carried out in the public interest or in the exercise of public powers (letter e), the basis of the treatment must be provided by Union law or the law of the member state, which in our case must be a norm with the status of law.

In addition, the processing of special categories of personal data (Article 9 RGPD) is permitted when: a. The treatment is carried out with the explicit consent of the interested party, unless the law of the Union or the member state does not allow it. b. The treatment is necessary to fulfill obligations or exercise rights in the workplace, if authorized by the law of the Union or the member state. c. The treatment is necessary to protect the vital interests of the data subject or one third party, if he does not have the capacity to consent.

d. The treatment is carried out in the scope of the legitimate activities of a non-profit organization with political, philosophical, religious or trade union purposes and refers to current or former members of the organization.

e. The treatment refers to data that the interested party has made manifest public

f. The treatment is necessary to formulate, exercise or defend claims or when the courts act in the exercise of their judicial function. g. The treatment is necessary for reasons of essential public interest. h. The treatment is necessary for the purposes of preventive and occupational medicine, medical diagnosis and provision and management of health care, on the basis of the law of the Union or a Member State or whenever the treatment is carried out by a subject health professional to professional secrecy or another person subject to the duty of confidentiality.

i. The treatment is necessary for reasons of public health on the basis of the right of the Union or a member state.

J. The treatment is necessary for archival purposes in the public interest, scientific or historical research or statistical purposes on the basis of the law of the Union or a member state.

Personal data relating to criminal convictions and offenses can only be processed under the supervision of public authorities or when authorized by Union or Member State law, which must establish adequate guarantees for the rights and freedoms of the data subjects (Article 10 GDPR).

When the legal basis that legitimizes the treatment is consent, which must be free, specific and unequivocal, the person concerned has the right to withdraw or revoke it in

Any moment. Withdrawal or revocation of consent does not have retroactive effects. Therefore, it does not affect the lawfulness of the treatment based on consent prior to withdrawal. On the other hand, withdrawing consent should be as simple as giving it.

IV

Apart from compliance with the principles, the RGPD foresees a series of obligations that the data controller must fulfill.

a) Keep a record of treatment activities

The GDPR has removed the obligation to notify the data protection supervisory authority of files for registration. However, it foresees new treatment documentation obligations for those responsible or in charge of the treatment, in particular, the need to keep a record of the treatment activities. The only exceptions to this obligation are those responsible or those in charge of the treatment with fewer than 250 workers. However, this exception does not apply if any of the following circumstances occur (art. 30.5 RGPDD): if there is likely to be a risk to the rights and freedoms of the affected subjects; if the treatment is not occasional; or if the processing includes special categories of data or relating to offenses and criminal convictions. In any case, this register must contain, with respect to each activity, the information established in article 30 of the RGPD.

APDCAT has developed a simple application to keep a record of processing activities so that those responsible and those in charge of processing (http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres).

b) Inform the interested parties

At the time of collecting the information, it is necessary to inform the interested persons about the conditions under which the processing of personal data is carried out (article 13 RGPD and 11 of the LOPDGDD), especially about the purpose or purposes for which the data will be processed.

The information must refer to:

- **The identity and contact details of the person in charge and, if applicable, of theirs representative**
- **The contact details of the data protection officer.**
- **The purposes and legal basis of the treatment.**
- **The recipients or categories of recipients of the data.**
- **The intention to transfer the data to a third country or an organization international and the basis for doing so, if applicable.**
- **The term during which the data or the criteria to be determined will be kept the**
- **The right to request access to the data, to rectify or delete it, to limit its processing, to oppose it and to request its portability.**
- **The right to withdraw at any time the consent that has been given.**
- **If the communication of data is a legal or contractual requirement or a requirement necessary to sign a contract, and if the interested party is obliged to provide the data and is informed of the consequences of not doing so.**

- **The right to submit a claim to a control authority, or, where applicable, before the Data Protection Officer.**
- **The existence of automated decisions, including the creation of profiles, and the information about applied logic and its consequences.**

This information must be given in an accessible and easy-to-understand form, with simple and clear language, especially when the information is addressed to a minor, indicating what this data is collected, used or treated for, as and as required by the GDPR. In this regard, it may be of interest to consult the Guide for the fulfillment of the duty to provide information in the RGPD (http://apdcat.gencat.cat/ca/documentacio/guies_basiques).

The LOPDGDD has foreseen the possibility of using a double-layer mechanism to comply with the information obligations, in such a way that the basic information that is relevant is provided, depending on whether the data has been obtained from the own interested person or a third party, with the possibility of forwarding to an email address or other means that allows the interested person to access the rest of the information provided for in the RGPD.

c) Processing orders to third parties or entities

In the case of dealing with third parties who provide services on behalf of the AFA and who process members' personal data, such as, for example, extracurricular activities, or manage the website or administrative activity, the corresponding ones must be signed contracts of those in charge of the treatment.

The RGPD expands the minimum content of the treatment order contract (article 28.3 RGPD and article 33 LOPDGDD). Among other aspects, the contract must provide for the following additional points with respect to the content already established by the LOPD: the purpose and duration of the assignment; the nature of the treatment; the type of personal data; the categories of interested persons; the obligations and rights of the person in charge; the provision that the persons who must treat the data undertake to maintain confidentiality; the assistance of the person in charge to the person in charge to deal with requests to exercise rights; the deletion or return of the data at the end of the order; the obligation to make available to the person in charge all the information necessary to demonstrate that he fulfills the obligations of the person in charge of the treatment and to allow and contribute to the person in charge or another auditor authorized by the person in charge carrying out audits and inspections

In this regard, it may be of interest to consult the Data Controller's Guide (http://apdcat.gencat.cat/ca/documentacio/guies_basiques/).

However, if you have a contract or processing order agreement signed before May 25, 2018, you should know that in accordance with the fifth transitional provision of the LOPDGDD, these remain valid until the indicated expiration date in the same When it comes to orders with an indefinite duration, they remain valid until May 25, 2022. In any case, during the validity of the contract or agreement, either party can demand from the other the modification of the contract to adapt the one established in article 28 of the RGPD.

d) Data Protection Officer

As a novelty, the RGPD introduces the figure of the data protection delegate, who can be part of the staff of the person in charge or the person in charge or act within the framework of a

service contract A data protection delegate must be appointed in the following cases: - When the treatment is carried out by a public authority or body (except for courts and tribunals). In this case, a single data protection officer may be appointed for several of these authorities or bodies.

- When the treatment requires the regular and systematic observation of interested parties a large scale
- When the treatment concerns special categories of personal data or data relating to convictions or criminal offences.

Given the treatments described in the consultation, it does not appear that the AFA must designate one. However, nothing prevents it from being designated voluntarily.

Once the delegate has been designated, the entities included in the scope of action of the APDCAT must communicate this designation to the Catalan Data Protection Authority. It is also necessary to keep the data communicated up to date.

Through the Authority's electronic headquarters https://seu.apd.cat/ca/tramits/DPD you can access the procedures to consult the designated DPDs or communicate the designation of the DPD.

e) Security measures

It is also necessary to adopt the technical and organizational measures appropriate to the risk involved in the processing of the data, to guarantee compliance with the regulations and protect the rights of the interested parties.

The RGPD does not establish any list based on the basic, medium and high security levels, as foreseen by the RLOPD, but leaves it to the discretion of the person in charge and the person in charge, after analyzing the risks, to determine which security measures will be implemented in each case.

From the point of view of information security, a risk analysis requires identifying the threats (for example, unauthorized access to personal data), assessing how likely it is to occur and the impact it would have on the people affected .

The type of risk and, in short, its probability and severity, varies according to the types of treatment, the nature of the data being treated, the number of interested persons affected, the amount and variety of treatments, the technologies used, etc.

In the case of treatments of little complexity, this analysis can be the result of a documented reflection on the implications of the treatments on the rights and freedoms of the persons concerned. This reflection must analyze the context in which the treatment is carried out (media, facilities, users, etc.) and must answer questions such as the type of data they deal with (special categories of data, col· vulnerable groups, of a large number of people, which allow the creation of profiles), if the disclosure, alteration or loss of the data may have significant consequences for the people affected, if the data is processed outside the equipment or installation locations of the person in charge, if third parties who provide services on behalf of the person in charge have access to the data, and particularly invasive technologies for privacy are used (geolocation, video surveillance, internet of things, etc.).

Therefore, it is very important that if a standard, easily auditable and objective methodology is not used, the issues that have been taken into account when determining the level of existing risk and specifying the security measures are documented in detail that must be applied. This will serve to comply with the principle of proactive responsibility.

However, this does not mean that the measures you applied following the RLOPD are not correct. Perhaps they are the right ones, but it is necessary, in any case, to carry out a risk analysis to determine if the measures implemented are sufficient or if there are any shortcomings. In any case, the selection of security measures must guarantee a level of protection appropriate to the risk.

v

Finally, for information purposes, the APDCAT has a catalog of resources to make compliance with the regulations easier.

Thus, you have at your disposal a set of regional, state and international regulations on data protection and other documents and tools of interest such as the APDCAT guides and the guidelines of the Working Group of the Article 29, in addition to other provisions adopted by the APDCAT (instructions, recommendations and other provisions). This information is available on the website: http://apdcat.gencat.cat/ca/autoritad/normativa

To inform you that, through the Authority's electronic headquarters https://seu.apd.cat, you can access the rest of the information, services and procedures that the Authority makes available to you, including others:

1.-Notify security breaches of personal data: this notification must be formalized using the notification form. Once the document has been generated in pdf format, with the electronically signed notification, it must be sent, together with the documentation that may be attached. If you are registered with EACAT you must submit the form using the generic submission of this platform; if not, you must submit it through E TRAM

2.-International transfers: in this section the AFA can process the following files: authorization of international data transfers and/or communication of international data transfers. The request must be formalized using the registration form. Once a pdf document has been generated with the electronically signed application, you can send it, together with the attached documentation, through ETRAM

3.-Request an opinion: through the president of the AFA, you can request an opinion from the Authority regarding a specific issue. The request must be formalized through the electronic headquarters.

4.-Propose a prior consultation: The data controller must make a prior consultation with the Catalan Data Protection Authority prior to the start of the treatment, among other cases, when an evaluation has been drawn up impact on data protection resulting in a high risk if the controller does not take measures to mitigate it. The request must be formalized using the registration form.

In addition, you have a personalized consulting service to provide ongoing support for all adaptation projects to personal data protection regulations that

perform To request the consulting service, you must address your request by email to: serveideconsultoria.apdcat@gencat.cat.

All of this without prejudice to the fact that you request other services made available by the APDCAT, such as the public assistance service that you can contact to request information or consult doubts in relation to the application of the legislation on the protection of personal data, or request information on courses, conferences, conferences, seminars and other training and outreach activities organized by the Authority or in which it participates. You can contact this service by email: atenciopublic.apdcat@gencat.cat.

In accordance with the considerations made in this opinion in relation to the query raised, the following are made,

Conclusions

The Authority values the effort on the part of the AFA in order to adapt to the data protection regulations, but considers that the document provided by the association and which it calls "Impact assessment relating to the protection of data" does not include the minimum content established by article 35.7 of the RGPD. In any case, this is not a mandatory document for the treatments described in the consultation.

In order to comply with data protection regulations, the AFA must comply with all the principles and obligations referred to in general terms in this report and any other established in Regulation (EU) 2016/679 , of the Parliament and of the European Council, of April 27, 2016, General Data Protection and Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Digital Rights.

Barcelona, February 20, 2019