CNS 3/2021

Opinion in relation to the query made by a body in relation to various applications to communicate with families who are using the municipal kindergartens

A query is presented to the Catalan Data Protection Authority from the data protection representative (DPD) of several councils assisted by the entity in relation to various applications to communicate with families who are using the homes municipal children.

In the consultation it is stated that to replace the communications of the agenda between the nursery and the parents, due to the current health situation, some homes have started to use various applications, including two applications (Dinantia and ClassDojo), of which the links are attached:

-https://www.dinantia.com/es/
-https://www.ClassDojo.com/ca-es/privacy/?redirect=true

He also explains that some home directors have stated that they had the approval of the education inspector for their use and that they are also being used in several public primary schools.

In this context, it requests the pronouncement of this Authority on the following issues:

"1. Does the use of these applications comply with data protection regulations?
2. In the case of clasdojo, which we think involves international data transfers, if you want to continue using it, is it necessary to request a prior report from the APDCAT?
3. Should an impact assessment be carried out before the use of these applications?
4.If you can continue using these applications, what are the main risks and what measures would be most appropriate to minimize them?
5 If you can continue using these applications, since you have the consent of the parents, is it possible to ask for consent without giving another alternative to communication with the school?

6. Who is responsible for the processing of the data stored by the app (the school or the companies that own these applications?"

In view of the consultation, a report has been requested from the technical area of this Authority in order to analyze the technical characteristics of these applications.

Having analyzed the query that is not accompanied by other documentation, and taking into account the report of the technical area, in accordance with the report of the Legal Counsel I issue the following opinion:

I

(...)

II

The inquiry that is the subject of this opinion refers to the use by certain municipal kindergartens of two applications to replace the agenda communications between the kindergarten and the parents.

In order to locate the query, it is necessary to describe, even if briefly, the two applications mentioned and their operation, based on the information available on the respective web pages: https://www.dinantia.com/es/ and https://www.ClassDojo.com/es-es/

The **Dinantia** application is defined as an application to manage communication in schools: between school and parents, and between school staff, and offers the following functionalities: *"publication of center notifications and reminders, request authorizations with digital signature, forms, attendance control, newsletter, communication reading control, reporting bullying".*

This application is offered in desktop and mobile versions. As stated on the website, if a center decides to use this application to communicate with parents or guardians, it is not necessary for them to download the application to their mobile phone, as communications can reach the parents' or guardians' email .

In any case, in its mobile version when a user downloads the application, Dinantia asks the user for permission to access the calendar, location, microphone, phone,
storage, and other permissions (run at startup, read pending alerts, view network connections, prevent phone from sleeping, receive internet data, read Google services settings, have access completed on the network, change audio settings etc.)

The application's privacy policy is not available on the web and, as far as we can see,
it is also not shown at the time of installing the application. You can only access the privacy policy and the data processing conditions of the website itself from the website. Therefore, it is unknown what data the application collects, its purpose, when it is saved, if it is shared with third parties, etc.

No information was found either on the location of the data storage that the application manages, or on the security measures it implements to protect the stored information. For example, it is not known what measures are applied to guarantee the confidentiality of the stored information (whether the information is kept in the clear or encrypted, etc.), nor is it known what security measures are applied to guarantee the availability and data integrity (if backups are made of the information managed by the educational centers and their frequency, etc.).

In relation to communications, no information has been found on the security measures they implement (it is not known if the communications are encrypted or made in the clear, it is not known if there is any technical measure to verify the identity of the person making the communication, etc.).

Regarding the development of the application, no information was found either (technology used, dependencies, etc.).

The **ClassDojo** app is a web and mobile app owned by a company based in the United States. According to the *"service conditions"* document, it offers the following services:

"- *Tools to help teachers and parents communicate with each other.*
- A way for teachers to give assignments and give feedback to students, and other tools to manage the class.
- A way for teachers to share photos, videos, files and other class information with parents and students.
- Student folders, with which students can share their work with teachers and parents.

- Activities and other content that teachers or parents want to share with students.
- A way for the school management to see the school community and communicate with parents."

This application can be used by schools for the different services it offers, although it is also offered as a tool for students or parents who, in particular, register as a learning tool. In the case of contracting the services of the platform by a school, it is the school itself that registers in the application and signs a contract with the supplier company for the provision of these services and registration in the parents' and students' application is done by the center itself, which can send the parents an invitation code. However, to be able to use all the functionalities, parents or guardians or even students need to download the mobile application.

It has been verified that ClassDojo has a very detailed data protection policy (written in English) which can be found at https://www.ClassDojo.com/ca-es/privacy. In which it is stated that it complies with the RGPD and other US data protection regulations: COPPA (Children's Online Privacy Protection Act) and FERPA (Family Educational Rights and Privacy Act). Compliance with the last two has been certified.

ClassDojo claims to collect the following information in its application, depending on the services it provides:

- First and last name
- Phone number
- Email address
- Password
- Mobile device ID
- Genre
- Age
- Information about the language
- Name of the school
- Address of the school
- Local identification number (school district)
- Geolocation data

• Photographs, videos, documents, drawings and/or audio files
• Students' class attendance data
• Feedback points
• IP address
• Browser details
• Access time
• Application usage time
• Functions used
• Source URL
• Clicks
• Activity time

Regarding information security, ClassDojo has a document (https://www.ClassDojo.com/ca-es/security/) detailing different aspects of security. Without intending to be exhaustive, the main aspects it covers are:

- Compliance with different security standards (ISO 27001, SOC 2, PCI DSS Level 1 and FISMA), which has been certified by external audits. There is no reference to the ENS.

- Encryption at rest and in transit. All data communications are encrypted (HTTPS protocol). ClassDojo also claims that it encrypts personally identifiable information (PII) when storing it. However, it is not clear whether this refers to all of a user's personal information or just information such as first and last name, phone number, email address, etc.).

- Data security vis-à-vis ClassDojo workers. Access is only given to people who need it for their work (engineers, data scientists, product managers and support staff). All access to your infrastructure is logged and passwords for access are secure and with multi-factor authentication.

- Data confidentiality. They seek to prevent unauthorized persons from gaining access to student data. (User identification and authentication procedures; ID/password security procedures; Encryption of archived data carriers; Encrypted data communications).

- Data integrity. The technical and organizational measures to control whether student data has been entered, changed or deleted and by whom.

- Availability of information, ClassDojo has measures such as geographically distributed backups, redundancy in technical means for data processing, etc.

The document also discusses other security measures such as those dedicated to ensuring the physical security of data processing facilities, the maintenance of treatment systems, etc.

In relation to data retention, ClassDojo specifies that if an account remains inactive for 12 months, it will be deleted. Some student account content will be retained after it is deleted for school legal compliance reasons (for example, the maintenance of

"educational records" under the Family Educational Rights and Privacy Act (FERPA)). The student's name originally provided by the teacher will remain, along with any submitted content such as photos and videos in the Student Story.

In this opinion, as requested in the consultation, we will focus on the use of the applications that are the subject of the consultation solely as a mechanism to replace the physical agenda in municipal kindergartens with the communication service they offer, although these applications, as explained, have many other functionalities, some of which are linked to learning, which will not be the subject of this opinion. In this sense, answers will be given to the different questions raised in the consultation, although the order of the questions will be altered for expository purposes.

III

Schools, and specifically in the case raised in the consultation, kindergartens, in the development of their activities process personal data of minors that require special consideration due to the situation of vulnerability of this group and the consequences which may arise from inadequate treatment of your information. Therefore, it is necessary to be extremely diligent in the treatment of this information.

In the specific case of communications between the school and parents or guardians through a communication system that offers agenda services, in the sense of allowing the school to inform parents or guardians about classroom activities or specific issues related to the minor and the response of the parents or guardians to these communications (which may include authorizations to carry out activities), and which also allows the parents to communicate to the center issues related to the minor as they may be the justification of non-attendance for health reasons, the need for the administration of some medicine, etc. involves the processing of personal data of both the student's parents or guardians, as well as data of the students themselves which, in some cases, may be special categories of data.

In order to answer the questions posed in the consultation, it must be taken into account that all data processing must comply with the principles and guarantees of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27 2016, General Data Protection (hereinafter, RGPD) and of Organic Law 3/2018, of December 5, Protection of Personal Data and guarantee of digital rights (LOPDGDD).

The RGPD articulates the protection of personal data through the principle of proactive responsibility according to which the data controller is responsible for compliance with the principles and guarantees provided for in the RGPD and, specifically, those contained in the first section of article 5 RGPD: legality, loyalty and transparency (Article 5.1.a), purpose limitation (Article 5.1.b), data minimization (article 5.1.c), accuracy (article 5.1.d), limitation of the retention period (article 5.1.e) and integrity and confidentiality (article 5.1.f). In accordance with this principle, the data controller must be able to demonstrate compliance.

Article 25 of the RGPD regulates the responsibility of the data controller in the following terms:

"1. Taking into account the nature, the scope, the context and the purposes of the treatment as well as the risks of varying probability and severity for the rights and freedoms of the physical persons, the person responsible for the treatment will apply appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the treatment complies with this Regulation. These measures will be reviewed and updated when necessary.

2. When they are provided in relation to the processing activities, among the measures mentioned in section 1 will be included the application, by the controller, of the appropriate data protection policies.

3. Adherence to codes of conduct approved in accordance with article 40 or a certification mechanism approved in accordance with article 42 may be used as elements to demonstrate compliance with the obligations of the controller."

"

Article 4.7 of the RGPD defines the controller as *the natural or legal person, public authority, service or other organism that, alone or together with others, determines the purposes and means of the treatment."*

Starting from the basis that the School (or, where appropriate, the City Council) is responsible for the processing of the personal data necessary for the exercise of its functions, whether educational and guidance or other related to the center's own activities .

Article 5.1.a) of the RGPD establishes that all processing of personal data must be lawful, fair and transparent in relation to the interested party (principle of lawfulness, loyalty and transparency).

In order for a treatment to be lawful, it is necessary to have, at least, a legal basis of those provided for in article 6.1 of the RGPD that legitimizes this treatment, either the consent of the person affected, or any of the other circumstances which provides for the same precept. In the field of public administrations, the legal bases provided for in letters c) and e) of article 6.1 of the RGPD are of particular interest, according to which the treatment will be lawful when it is necessary for the fulfillment of 'a legal obligation applicable to the controller (letter c), or when the treatment is necessary for the fulfillment of a public interest or in the exercise of public powers conferred on the controller (letter e).

Article 6.3 of the RGPD establishes that the basis of the treatment indicated in article 6.1. c) and e) must be established by the Law of the European Union or by the law of the Member States that applies to the data controller. The reference to the legitimate basis established in accordance with the internal law of the Member States referred to in this article requires that the rule of development, when dealing with the protection of personal data of a fundamental right, has the status of law (Article 53 EC), as Article 8 of the LOPDGDD has come to recognize.

Regarding the processing of students' personal data, the twenty-third additional provision of Organic Law 2/2006, of May 3, on Education, establishes:

"Personal data of students.

1. Educational centers may collect the personal data of their students that are necessary for the exercise of their educational function. These data may refer to

origin and family and social environment, to personal characteristics or conditions, to the development and results of their schooling, as well as to those other circumstances whose knowledge is necessary for the education and orientation of the students.

2. The parents or guardians and the students themselves must collaborate in obtaining the information to which this article refers. The incorporation of a student in a teaching center will involve the treatment of his data and, in his case, the transfer of data from the center in which he had previously studied, in the terms established in the legislation on data protection. In any case, the information referred to in this section will be strictly necessary for the teaching and guidance function, and cannot be used for purposes other than education without express consent.

3. In the treatment of student data, technical and organizational rules will be applied that guarantee their security and confidentiality. The teaching staff and the rest of the staff who, in the exercise of their functions, access personal and family data or which affect the honor and privacy of minors or their families will be subject to the duty of secrecy.

4. The transfer of data, including those of a reserved nature, necessary for the educational system, will preferably be carried out electronically and will be subject to the legislation on the protection of personal data.

In the case of the transfer of data between Autonomous Communities or between these and the State, the minimum conditions will be agreed by the Government with the Autonomous Communities, as part of the Education Sectoral Conference."

Therefore, the LOE enables educational centers, whether public or private, to process the personal data of their students that are necessary for the exercise of their educational and guidance function.

The second section of the provision of the aforementioned LOE refers to the collaboration of parents, guardians and the students themselves in obtaining this information. Therefore, in the scope of its educational and guidance function, the center is able to process the personal data that is necessary for both the student and the parents or guardians. Outside of these cases, the legal basis of the treatment may be consent or another basis of those provided for in article 6.1 RGPD, in accordance with the requirements established in the RGPD.

It is also appropriate to take into account the modification introduced to the LOE by Organic Law 3/2020, of December 29, specifically the introduction of a new article 111 bis which establishes:

"1. The Ministry of Education and Professional Training will establish, after consultation with the Autonomous Communities, the standards that guarantee interoperability between the different information systems used in the Spanish Educational System, within the framework of the National Interoperability Scheme provided for in article 42 of the Law 11/2007, of June 22, on electronic access for citizens to Public Services.

(...)

"As part of the implementation of the aforementioned measures, within the information systems proper to academic and administrative management, an identification number will be regulated for each student, in order to facilitate the exchange of relevant information, the follow-up of individualized educational trajectories, including the educational measures that could have been applied in their case, and to meet the demands of state and international statistics and European strategies for education and training systems. In any case, said regulation will comply with the regulations relating to privacy and protection of personal data.

2. ***The virtual learning environments that are used in teaching centers supported with public funds will facilitate the application of specific educational plans designed by teachers to achieve specific curriculum objectives, and must contribute to the extension of the classroom concept in the time and space.*** *Therefore, respecting the standards of interoperability, they must allow students access, from any place and at any time, to the learning environments available in the teaching centers where they study, with full respect for the provisions of the applicable regulations on intellectual property, privacy and personal data protection. Likewise, they will promote the principles of universal accessibility and design for all people, both in formats and content and in tools and virtual learning environments.*

3. The Ministry of Education and Professional Training will promote, after consultation with the Autonomous Communities, the compatibility of formats that can be supported by tools and virtual learning environments in the field of public digital educational content, with the aim of facilitating their use regardless of the technological platform in which they are housed.

(...)

5. The educational administrations and the management teams of the centers will promote the use of information and communication technologies (ICT) in the classroom as an appropriate and valuable didactic medium to carry out teaching and learning tasks. The educational administrations must establish the conditions that make possible the elimination in the school environment of the situations of risk derived from the inappropriate use of ICT, with special attention to the situations of violence in the network. Confidence and security in the use of technology will be promoted, paying special attention to the disappearance of gender stereotypes that make it difficult to acquire digital skills under conditions of equality.

6. The Ministerio de Educación y Formación Profesional will draw up and review, after consultation with the Autonomous Communities, the frameworks of reference for digital competence that guide the initial and permanent training of teachers and facilitate the development of a digital culture in the centers and in the classrooms

7. The public administrations will ensure that all students have access to the necessary digital resources, to guarantee the exercise of the right to education for all boys and girls under equal conditions.

In any case, the information and communication technologies (ICT) and the teaching resources that are used will conform to the regulations governing information services and society and intellectual property rights, raising awareness of the respect of the rights of third parties.

Also in this sense, article 83 of the LOPDGDD establishes the following:

"1. The educational system will guarantee the full insertion of students in the digital society and learning to use digital media in a safe and respectful manner human dignity, constitutional values, fundamental rights and, particularly with the respect and guarantee of personal and family privacy and the protection of personal data. The actions carried out in this area will have an inclusive character, in particular with regard to students with special educational needs.

The educational administrations must include in the design of the block of subjects free configuration of the digital competence referred to in the previous section, as well as the elements related to the risk situations derived from the inadequate use of ICT, with special attention to situations of online violence.

2. The teaching staff will receive the digital skills and the necessary training for it teaching and transmission of the values and rights referred to in the previous section.

3. The study plans of the university degrees, especially those that qualify for professional performance in student training, they will guarantee training in the use and security of digital media and in the guarantee of fundamental rights on the Internet.

So, and taking into account this mandate to promote digital skills and the use of virtual learning environments, it can be considered that the processing of students' data for this purpose would have a legal basis in that it is a mission in the public interest (according to article 6.1.e) of the RGPD with the requirements of the LOPDGDD and the LOE.

IV

Starting with the sixth question that arises, it is necessary to determine, first of all, whether the person responsible for the processing of the data used or stored by the applications is the school or the companies that own these applications. It is therefore appropriate to analyze the relationship between the school and the company supplying the applications.

According to article 4.7 of the RGPD, the person responsible for the treatment is the one who establishes the purpose or the result of the treatment (in this case it could be to maintain communication with families for educational purposes in times of pandemic); decide on the purpose and uses of the information; and decides on the means of treatment (in this case the services offered by an external company that provides them with an IT application).

Article 4.8 of the RGPD defines the person in charge of the treatment, as *"the natural or legal person, public authority, service or other organism that treats personal data on behalf of the person responsible for the treatment".*

The decision on whether the person responsible for the treatment is the school (the school management) or the City Council to which it depends, is an organizational issue that will have to be determined based on who actually has, in the case at hand, the capacity to decision on the mentioned aspects.

In any case, the company that provides the service of platforms accessible via the Internet, to the extent that it has access to personal data to provide this service, or treats it in any other way (art. 4.2 RGPD), will have the consideration of the person in charge of the treatment.

The person in charge of the treatment must choose a person in charge of the treatment that offers sufficient guarantees regarding the implementation and maintenance of appropriate technical and organizational measures, in accordance with the provisions of the RGPD, and that guarantees the protection of the rights of the affected persons (Article 28.1 RGPD). Therefore, there is a duty of care when choosing th in charge of the treatment.

This assignment must be formalized through a contract or other legal act subject to the law of the Union or of the member states which must regulate the aspects provided for in article 28.3 of the RGPD:

"
The processing by the controller will be governed by a contract or other legal act in accordance with the Law of the Union or the Member States, which binds the controller with respect to the controller and establishes the object, duration, nature and purpose of the processing, the type of personal data and categories of interested parties, and the obligations and rights of the person in charge. Said contract or legal act will stipulate, in particular, that the manager:

a) will treat personal data solely following the documented instructions of the person in charge, including with respect to transfers of personal data to a third country or an international organization, unless it is obliged to do so by virtue of the Law of the
Union or Member States that applies to the person in charge; in such a case, the manager will inform the person in charge of that legal requirement prior to the treatment, unless such Law prohibits it for important reasons of public interest;

b) will guarantee that the persons authorized to treat personal data have committed to respect confidentiality or are subject to a confidentiality obligation of a statutory nature;

c) will take all the necessary measures in accordance with article 32;

d) will respect the conditions indicated in sections 2 and 4 to resort to another treatment manager;

e) will assist the person in charge, taking into account the nature of the treatment, through appropriate technical and organizational measures, whenever possible, so that he can comply with his obligation to respond to requests aimed at the exercise of the rights of the interested parties established in chapter III;

f) will help the manager to ensure compliance with the obligations established in articles 32 to 36, taking into account the nature of the treatment and the information available to the manager;

g) at the choice of the person responsible, will delete or return all personal data once the provision of the treatment services is finished, and will delete the existing copies unless the conservation of personal data is required under Union Law or member states;

h) will make available to the person in charge all the information necessary to demonstrate compliance with the obligations established in this article, as well as to allow and contribute to the performance of audits, including inspections, by the person in charge or another auditor authorized by said responsible."

Therefore, the data controller, in order to use these applications, must sign a contract or other legal document that binds the company that owns these applications and guarantees that it meets the requirements of the RGPD and, in specific each of the aspects collected in the third section of article 28 of the RGPD.

In the case of application providers, as in the case of the ClassDojo application, it is common for them to offer general service acceptance clauses, which must be assessed by the data controller to determine whether they allow all requirements to be met and guarantees referred to in article 28.3 of the RGPD.

v

The fifth question asks if it is possible to ask for parental consent without giving another alternative to communication with the school. In this regard, it must be said that, if the use of the applications is carried out in the context of communication with parents linked to the exercise of educational and guidance functions, the legal basis for this treatment could be, as as explained, article 6.1.e) of the RGPD in relation to the LOE.

However, nothing prevents the school from deciding to use a particular tool based on consent alone, so that it uses a communication tool only with consenting parents. In this sense, article 4.1 RGPD establishes that consent is understood as *"any free, specific, informed and unequivocal manifestation by which the interested party accepts, either through a statement or a clear affirmative action, the treatment of personal data that concern him".*

At the outset, and as stated in Opinion 02/2013 of the Article 29 Working Group on the applications of smart devices, which analyzes the adequacy of data protection regulations, the development of applications in devices and which includes recommendations for both developers and users, it is necessary to differentiate between consent prior to the installation of an application, from the legal basis for the processing of personal data. Although this Opinion predates the RGPD, the considerations it contains are still valid in many respects.
Thus point 3.4.1 establishes:

"3.4.1 Prior consent to the installation and processing of personal data In the case of applications, the main applicable legal basis is consent.
When you install an application, information is entered on the end user's device. Many applications also access data stored on the device, the contact list, photographs, videos and other personal documentation. In all these cases, article 5, section 3, of the Directive on electronic privacy requires the consent of the user after clear and complete information has been provided, before the introduction and extraction of data from the device.

It is appropriate to observe the distinction between the consent required to enter or read information on the device and the consent necessary to have a legal basis for the treatment of different types of personal data."

In this case it is necessary to distinguish between the consent that parents or guardians must give in order to install the application on your devices, and consent as a legal basis for processing your personal data, which must meet the requirements of the RGPD and, therefore, must be informed about all aspects related to the processing of personal data as a result of using the application for the purpose of communicating with the school.

With regard to consent as a legal basis for the processing of data by public administrations, it must be taken into account that according to the RGPD, consent has not been given freely when there is a clear imbalance between the interested party and the person in charge of the treatment, so recital 42 RGPD makes it clear that *To guarantee that the consent has been given freely, this should not constitute a valid legal basis for the treatment of personal data in a concrete case in which there is a clear imbalance between the interested party and the person responsible for the treatment, in particular when said person responsible is a public authority and it is therefore unlikely that consent has been given freely".*

However, this does not mean that consent cannot be a legitimate basis for data processing carried out by a public administration. Thus, as stated by the Working Group of Article 29 in the Guidelines on consent in the sense of Regulation (EU) 2016/679, a public school can request consent for the publication of images of its students in a school magazine. As the aforementioned document concludes, consent in these situations would be a valid legal basis as long as *"the students were not denied education or other services and they could refuse the use of said photographs without suffering any harm".*

In any case, consent must be free. Therefore, it can be concluded that in general consent can only be an appropriate legal basis if control is offered to the data subject and he has a real choice to accept or reject the terms offered to him without suffering any prejudice as as a result of not giving your consent.

Consequently, if the use of these tools is to be based on parental consent, and given that communication with parents can be considered to be necessarily part of the content of the educational and guidance function of the educational centers, it will be necessary to have alternatives to be able to follow the school's agenda and communications, without this causing them harm.

VI

The need to carry out a privacy impact assessment prior to the use of these applications is analyzed below, in response to question number three made in the consultation. This question is closely related to the fourth question about what are the main risks and what measures would be most appropriate in order to minimize them.

Regardless of the fact that in any data processing it is necessary to carry out an analysis of the risks involved in the processing (recital 76, *"The risk must be weighed on the basis of an objective evaluation through which it is determined whether the operations of data processing suppose a risk or if the risk is high") ,* paragraph 1 of article 35 of the RGPD establishes, in general, the obligation of the person in charge of data processing to carry out an impact assessment related to data protection (AIPD), with a character prior to the start of the treatment, when it is likely that due to their nature, scope, context or purposes they entail a high risk for the rights and freedoms of natural persons, a high risk which, according to the RGPD itself, is seen increased when the treatments are carried out using *"new technologies".*

The same article 35.3 of the RGPD specifies that, among other cases in which it derives from the provisions of the first section, an impact assessment relating to data protection must be carried out in the following cases:

"a) systematic and comprehensive evaluation of personal aspects of physical persons that is based on automated processing, such as profiling, and on the basis of which decisions are made that produce legal effects for physical persons or that significantly affect them in a 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, or

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

The data processing of the case at hand does not seem to be able to fit into any of the cases referred to.

Thus, with regard to the first assumption, it does not respond to a systematic and comprehensive evaluation of personal aspects of natural persons based on automated processing, such as profiling.

With regard to the second and third cases, to define what is to be understood by *"large-scale processing",* document WP 243 *"Guidelines on Data Protection Delegates (DPDs)"* of the Working Group of the Article 29, which considers that the following must 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 data processed, the duration or permanence of the treatment activity, the geographical extension of the treatment activity. Thus, and in accordance with the guidelines of the GT29, insofar as the main purpose of the treatment is not the communication of special categories of data and that its treatment can be considered occasional, it can

rule out in principle that there is in this case a large-scale treatment of special categories of data.

It should also be taken into account that article 35.4 of the RGPD establishes that *"the control authority will establish and publish a list of the types of processing operations that require an impact assessment related to data protection in accordance with section 1. "*
In accordance with this, this Authority, following the Guidelines established by the Working Group of article 29 in the aforementioned document WP 248, and the criteria for the assessment of the greatest risk provided for in article 28.2 of the LOPDGDD, has drawn up and published on the APDCAT website a list of types of data processing that require an impact assessment related to data protection).

Thus, when analyzing data treatments, it will be necessary to carry out an impact assessment related to data protection in most cases where this treatment complies with two or more criteria from the list, unless the treatment is in the list of treatments that do not require impact assessment referred to in article 35.5 of the RGPD (so far this Authority has not published any list with exclusions for the purposes of article 35.5).

It is therefore appropriate to analyze whether two or more of the criteria in the list are met in the case raised in the query. Section 4 of the list refers to: *"Treatments that involve the use of special categories of data referred to in article 9.1 of the RGPD" .* It should be taken into account that schools can process special categories of minors' data, such as health data, racial origin, etc. by virtue of the educational and guidance functions attributed to them by the LOE. However, it should be borne in mind that the inclusion of this type of information in the agenda or communications with parents should only have a very occasional character, in no case qualifying as large-scale. Therefore, in principle if the treatment carried out only involves the occasional collection of these special categories of data necessary for the educational functions, it does not seem that an impact assessment relating to the data protection, taking into account, in addition, that they would be collected in compliance with legal obligations and that they would affect a limited number of people.

Section 9 of the list refers to *"Data processing of vulnerable subjects or at risk of social exclusion, including data of children under 14 years of age, adults with some degree of disability, disabled people, people who access social services and victims of gender violence, as well as their descendants and people who are under their guard and custody"* and apparatus 10 a
"Treatments that involve the use of new technologies or an innovative use of established technologies, including the use of technologies on a new scale, with a new objective or combined with others, so that it involves new forms of data collection and use with risk for people's rights and freedoms.". Both criteria seem to be applicable in the case at hand.

Therefore, although the special categories of data may be dealt with in the application only occasionally, the fact that they affect minors and that a technology is used for which there is not much information about its operation and the risks it may entail, they do
at least recommended, in light of the principle of proactive responsibility (art. 5.2 RGPD), to carry out an impact assessment related to data protection.

In this sense, to carry out the impact assessment it is recommended to take into account the Practical Guide on the AIPD, of this Authority, available on the website www.apdcat.cat. On the Authority's website you can also find and download an app to do the assessment

It should be taken into account, finally, that if after having carried out the AIPD it turns out to be a high-risk situation that has not been mitigated, a prior consultation with the Catalan Data Protection Authority must be considered, which must be accompanied by a copy of the AIPD (art. 36 RGPD).

In any case, and answering not only the third question but also the fourth question included in the consultation, it will be in view of this impact assessment, which will be able to determine what the existing risks are and what measures can be adopted to mitigate them.

In any case, special attention must be paid to the fact that these applications can use a *"Cloud Computing"* model . In *"Cloud Computing"* the data is hosted in the service provider in the cloud and the services are accessed via the Internet from any device (mobile phone, personal computer, tablet). In this model, the main risks arising from the treatment are related to the correct implementation of security measures that prevent the alteration, loss, treatment or unauthorized access to the data, to the implementation of measures that guarantee the holders of the data obtain information on the treatment and exercise of rights and the control of your data. Likewise, in this model the service provider can be anywhere in the world, and therefore one of the main risks is that international transfers of minors' data occur, an issue that is analyzed in the legal basis below.

VII

In order to answer the second question, regarding the possible international transfers of data carried out by one of the applications, it must be taken into account that an international transfer of data occurs when the personal data processed by a person in charge or a processor in the European Economic Area are sent to a third country or international organization outside this territory.

The RGPD includes the regime applicable to international transfers in articles 44 to 49 which includes the regulation of the mechanisms that make it possible to ensure that the destination of the data to be transferred offers an adequate level of protection in relation to what guaranteed by the GDPR.

According to the RGPD, data can only be communicated outside the European Economic Area when the European Commission has adopted a decision that recognizes specific countries, territories or sectors (the RGPD also includes international organizations) that offer a adequate level of protection (Article 45 RGPD)

In the absence of an adequacy decision, it is possible to carry out international transfers without any express authorization when adequate guarantees have been offered regarding the protection that the data will receive at its destination, through one of the instruments provided for in article 46.2 RGPD:

"a) a legally binding and enforceable instrument between authorities or public bodies;

b) binding corporate rules in accordance with article 47;

c) type of data protection clauses adopted by the Commission in accordance with the examination procedure referred to in article 93, section 2;

d) data protection type clauses adopted by a control authority and approved by the Commission in accordance with the examination procedure referred to in article 93, section 2;

e) a code of conduct approved in accordance with article 40, together with binding and enforceable commitments of the person responsible or the person in charge of the treatment in the third country to apply adequate guarantees, including those relating to the rights of the interested parties, or

f) a certification mechanism approved in accordance with article 42, together with binding and enforceable commitments of the person in charge or the person in charge of the treatment in the third country to apply adequate guarantees, including those relating to the rights of the interested parties

It is also possible to carry out transfers with the authorization of a Control Authority, in this case the APDCAT, based on the guarantees provided through the instruments provided for in paragraph 3 of article 46, as follows:

"a) contractual clauses between the person in charge or the person in charge and the person in charge, person in charge or recipient of the personal data in the third country or international organization, or

b) provisions that are incorporated into administrative agreements between authorities or public bodies that include effective and enforceable rights for those interested."

Apart from these cases, article 49 RGPD establishes exceptions that allow data to be transferred without any of the previous mechanisms when any of the circumstances it provides for, among which the interested party has expressly given their consent to the proposed transfer. It must be taken into account, however, that in accordance with paragraph 4 of article 49, it is excluded that the transfer can be based on the possibility provided for in letters a), b) and) relating respectively to the consent of the interested party, the transfer is necessary for the execution of a contract, or the conclusion or execution of a contract in the interest of the interested party, with respect to the activities carried out by the public authorities in the exercise of their public authorities

In other words, the international transfer cannot be based on the consent of the interested parties regarding the activities carried out by the public authorities in the exercise of their public powers.
Therefore, if the city council bases the treatment on the exercise of its educational and guidance functions attributed to it by the LOE, the international transfer of the parents' data cannot be based on their consent.

For the transfer of data to countries that do not guarantee an adequate level of protection, the controller must certify that the processor is in a position to offer adequate guarantees. In any case, it must guarantee that the interested parties have enforceable rights and effective legal actions.

In the case at hand, the ClassDojo application transfers data to the United States.
It should be taken into account that the Executive Decision 2016/1250 of the Commission, of July 12, 2016, in accordance with Directive 95/46/EC of the European Parliament and of the Council, on the adequacy of the protection conferred by the EU-EE Privacy Shield, has been invalidated by Judgment C-311/18 (Schrems II), of the Court of Justice of the European Union (CJEU) of July 17, 2020.

Therefore, from the mentioned Judgment, international transfers of data to the United States cannot be carried out on the basis of the Privacy Shield, having been invalidated by the CJEU, considering that the United States is a third country that does not offer a adequate level of protection.

In the absence of an adequacy decision, the recommendation of the European Data Protection Committee of November 10, 2020 *"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data",* gathers tools so that data exporters can, in line with what is gathered from the Judgment of the European Court of Justice that invalidates the privacy shield, be able to guarantee that the level of protection in third countries is *"essentially equivalent"* to that guaranteed in the European economic area.

In this context, regarding the DPD's question: *"In the case of clasdojo, which we think involves international data transfers, in the case of wanting to continue using it, is it necessary to request a prior report from the APDCAT?"* The answer is that if one of the mechanisms provided for in the RGPD is not available to provide adequate guarantees or one of the exceptions applicable to public administrations does not apply, these transfers cannot be made.

VIII

Finally, by way of conclusion and giving an answer to the first question of the query, it is necessary to determine whether the use of the mentioned applications complies with the data protection regulations. In order to do so, and aside from the considerations that have already been made regarding the specific aspects discussed, it is necessary to mention some additional issues:

Taking into account the specific area in which the treatment would be carried out, it must be taken into account that Opinion 02/2013, of February 27, 2013, on the applications of smart devices, of the Working Group of the article 29 (GT29), includes among the obligations of application developers to comply with data protection regulations. These obligations include providing a readable, understandable and easily accessible privacy policy that informs consumers, at a minimum, about: who is responsible

(identity and contact details); the categories of personal data that the application will collect and process; what the data will be processed for; if the data will be communicated to third parties with specific indication to whom they will be communicated; the rights they have with respect to their personal data, as well how to allow the exercise of these rights and the mechanisms to exercise them; define a reasonable period of retention of the data collected by the application and establish a period of inactivity past which the account is considered expired. In short, GT29 determines that this information should be easily accessible in the privacy policy of the application, consequently if any of these aspects are missing or when the information provided does not offer adequate guarantees, the congruent recommendation would be that of do not use the application.

Regarding the Dinantia application, as far as we have been able to verify, there is no information published on its website about the privacy policy.

Regarding the ClassDojo application, the privacy policy on its website is written in English and it has not been possible to verify that when a user downloads the application, they have the specific information about the privacy policy that is applies to your data in an accessible and understandable way.

What has been verified is that the published privacy policy incorporates a document called the CLASSDOJO STUDENT DATA PRIVACY ADDENDUM, which aims to regulate the contractual relationship between the schools and the company providing the application in in relation to the processing of students' personal data.

This document is structured in 7 points or agreements, the seventh of which regulates the additional provisions that apply to schools located in the European Economic Area and therefore the RGPD applies to them, this addendum is analyzed below for centers located in the EEA.

The first section of this seventh agreement, under the title in English *"Roles",* establishes that the school is responsible for the treatment and designates the supplier company as responsible for the treatment of the students' data. Transparency regarding this distribution of roles is positively valued.

The second section under the title in English *"Scope"* indicates the scope of the agreement which it says applies to the processing of data by the provider on behalf of the center and in accordance with the instructions given by the latter in relation to contracted services. (refers to Annex B which includes the subject matter, the purpose of the treatment and the data and data categories of the student).

It has been verified that there is an annex A that describes the services offered and a very detailed annex B that specifies all the data that is collected, in this annex it is referred to a web page https://www.ClassDojo.com/transparency to obtain information on: the categories of data collected depending on the different user profiles (student, teacher, parents, etc.) the nature and purpose of the data processing activities, the country where the data is stored , the list of special categories of data collected (indicated that they are not collected at this time). A web page with the company's current list of service providers is also listed.

The third point under the English title *"Instructions",* regulates that the provider must only process the student's data according to the documented instructions given by the center and the prohibition to process the data for a purpose other than established It is expected that the instructions are those set out in the agreement although the center may issue additional instructions if it considers it necessary to comply with data protection regulations, it specifies who are the authorized persons to give instructions (center management, delegate of data protection or manager of the center's legal department). The possibility of giving instructions in relation to the contractor, beyond those set out in the agreement, is positively valued given that it is one of the functions of the data controller and must be in writing in the contract.

The fourth point under the title in English *"Subprocessing",* regulates the authorization of the center to the provider to hire the sub-processors listed in the list of service providers with the commitment that it will collect sufficient guarantees from all the sub-processors
implement the technical and organizational measures to comply with data protection regulations and the agreements in this document. There is, however, no list of subcontracted companies that allows the person in charge to know if there are any and which ones they are. With respect to this provision, it is important that the center has the ability to oppose certain companies acting as sub-processors if they consider that they do not sufficiently guarantee compliance with data protection regulations.

The fifth point regulates international data transfers, this clause provides that, the school authorizes the provider to carry out international data transfers to countries subject to a current adequacy decision of the European Union Commission and to carry out the data transfers listed in annex b. Specifically, the provider undertakes to maintain a privacy shield certification. This aspect cannot currently be considered sufficient, taking into account what has already been set out in ground VII of this opinion.

The sixth point under the title in English *"Personnel",* regulates the obligation of the provider to implement the appropriate technical and organizational measures to ensure that the staff processes the data in accordance with the instructions of the data controller and refers to the sections of the agreement that regulates the obligations, access passwords and employee training.

The seventh point under the English title *"Confidentiality",* regulates the provider's obligation to keep student data and any information related to the treatment with strict confidentiality.

The eighth point under the English title *"Security and Personal Data Breaches"* establishes that the provider has the obligation to implement technical and organizational measures to guarantee a level of security appropriate to the risks that the treatment may offer, including encryption and the pseudonymization of student data as established in the section of the agreement corresponding to data security. An external auditor certifies compliance with security standards such as: ISO 27001, SOC 2, PCI DSS Level 1 and FISMA.

It should be taken into account, however, that the municipality holding the data is subject to compliance with the National Security Scheme (ENS) in accordance with the provisions of the first additional provision of the LOPDGDD. In the case under analysis, although ClassDojo has a document on its website (https://www.ClassDojo.com/ca-es/security/) detailing different aspects of security, as collected in legal basis II of this opinion, it has not been possible to verify that the supplier complies with all the security measures derived from the ENS.

With regard to security breaches, it states that the provider must inform the center without undue delay after becoming aware of a data security breach and is subject to the procedure established in the apparatus of the agreement that regulates the breaches

The ninth point under the English title *"Assistance"* states that the supplier must provide reasonable assistance to the school in fulfilling the obligations of the data protection regulations regarding: 1) the fulfillment of requests to exercise the rights of
interested parties, 2) respond to inquiries or complaints from data holders 3) respond to

investigations and inquiries of the control authorities, 4) notifying personal data breaches of the school's student data, and 5) prior consultations with Control Authorities Collect the provider's commitment to inform the school if it believes that a instruction violates data protection regulations. The obligations to guarantee the exercise of the rights of the interested parties are complied with. However, there is a lack of provision regarding the submission to the audits determined by the person in charge or, at least, the knowledge on the part of the person in charge of the independent audits to which the platform is subjected.

This section also contains a provision to the effect that, unless it is prohibited by the EU or the laws of the EU member states and subject to a specific procedure, the provider must immediately inform the school center if it receives a single law enforcement, the courts or any government or any entity, to access personal data and, in any case, it is expressly provided that if "If Provider is prevented from notifying LEA as required under or this DPA, Provider must consult and comply with the instructions of the competent Supervisory Authority".

Although the fourth pact of the privacy addendum provides that the provider must delete all the student's data when requested by the school, there is a lack of concreteness regarding the fate that will be given to the data once the task of processing in this seventh agreement has been completed.

Therefore, it can be concluded that the use of this application cannot be guaranteed to comply with data protection regulations given the shortcomings analyzed relating, among others, to having an easily accessible and understandable privacy policy, to offer sufficient guarantees with regard to international data transfers, to guarantee compliance with the security measures of the ENS or that the data controller can object to the outsourcing of services to third-party companies.

Conclusions

The educational center or, as the case may be, the town hall to which the kindergarten depends, is responsible for the processing of the students' and parents' data, while the companies providing the applications that are the subject of the consultation would be in charge of the processing of 'this data.

The use of applications for communication with parents linked to the exercise of educational and guidance functions can be covered in article 6.1.e) in relation to the provisions of the LOE. In the event that the treatment is to be based on consent, in order for this to be valid, parents must have alternatives to be able to follow the school's agenda and communications, without this entailing harm .

The main risks arising from the use of these applications are related to the correct implementation of security measures that prevent the alteration, loss, treatment or unauthorized access to the data, to the implementation of measures that guarantee the holders of the data obtain information about the treatment and exercise of rights and the control of your data, especially those arising from the use of cloud computing and the international transfer of data.
For these purposes and to identify and, where appropriate, mitigate existing risks, it is highly recommended to carry out an impact assessment relating to data protection.

With regard to the query on whether the use of these applications complies with the data protection regulations, it must be taken into account that the person responsible for the treatment must choose a person in charge of the treatment that offers sufficient guarantees regarding the implementation and maintenance of the technical measures and appropriate organizational measures, in accordance with what is established by the RGPD, and which guarantees the protection of the rights of the persons affected.

With the information provided and that which has been obtained from the Internet, there is not enough data to determine whether the Dinantia application offers the necessary guarantees that are required of a data controller.

Regarding the ClassDojo application, although the information offers greater guarantees of compliance with the RGPD than that obtained in the case of Dinantia, there are certain shortcomings, specified in the legal foundations VII and VIII of this opinion, which prevent us from concluding on the basis of the information available, the suitability to the RGPD.

Barcelona, February 25, 2021