CNS 3/2021

Dictamen en relació amb la consulta formulada per un organisme en relació amb diverses aplicacions per comunicar-se amb les famílies que estan utilitzant les llars d'infants municipals

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta de la delegada de protecció de dades (DPD) de diversos ajuntaments assistits per l'entitat en relació amb diverses aplicacions per comunicar-se amb les famílies que estan utilitzant les llars d'infants municipals.

En la consulta s'exposa que per substituir les comunicacions de l'agenda entre la llar d'infants i els pares, degut a la situació sanitària actual, algunes llars han començat a utilitzar aplicacions diverses, entre les quals dues aplicacions (Dinantia i ClassDojo), de les quals adjunten els links:

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

També explica que alguns directors de les llars han manifestat que disposaven de la conformitat de l'inspector d'ensenyament per la seva utilització i que també s'estan utilitzant en diversos col·legis públics de primària.

En aquest context sol·licita el pronunciament d'aquesta Autoritat sobre les qüestions següents:

"1.La utilització d'aquestes aplicacions compleix la normativa de protecció de dades?
2. En el cas de clasdojo, que pensem que comporta transferències internacionals de dades, en el cas de voler continuar amb la seva utilització, cal demanar informe previ a l'APDCAT?
3.Caldria fer una avaluació d'impacte, abans de la utilització d'aquestes aplicacions?
4.De poder continuar utilitzant aquestes aplicacions, quins són els principals riscos i quines mesures serien més adients per tal de minimitzar-los?
5 De poder continuar utilitzant aquestes aplicacions, ja que es té el consentiments dels pares, és possible demanar el consentiment sense donar una altra alternativa a la comunicació amb l'escola?
6.Qui és el responsable del tractament de les dades que emmagatzema les app (l'escola o les empreses titulars d'aquestes aplicacions?"

A la vista de la consulta s'ha demanat informe a l'àrea tècnica d'aquesta Autoritat per tal d'analitzar les característiques tècniques d'aquestes aplicacions.

Analitzada la consulta que no s'acompanya d'altra documentació, i tenint en compte l'informe de l'àrea tècnica, d'acord amb l'informe de l'Assessoria Jurídica emeto el dictamen següent:

I

(...)

II

La consulta objecte d'aquest dictamen fa referència a la utilització per part de determinades llars d'infants municipals de dues aplicacions per substituir les comunicacions de l'agenda entre la llar d'infants i els pares.

Per tal de situar la consulta, cal descriure, encara que sigui breument, les dues aplicacions citades i el seu funcionament, en base a la informació disponible en les respectives pàgines web: https://www.dinantia.com/es/ i https://www.ClassDojo.com/es-es/

L'aplicació **Dinantia** es defineix com una aplicació per gestionar la comunicacions en les escoles: entre escola i pares, i entre personal de l'escola, i ofereix les funcionalitats següents: "*publicació de notificacions del centre i recordatoris, sol·licitud d'autoritzacions amb signatura digital, formularis, control d'assistència, newsletter, control de lectura de les comunicacions, denuncia de bullying".*

Aquesta aplicació s'ofereix en versió per a ordinador i mòbil. Tal com es fa constar en el web si un centre decideix utilitzar aquesta aplicació per comunicar-se amb els pares o tutors no és necessari que aquests es descarreguin l'aplicació al seu mòbil ja que les comunicacions poden arribar al correu electrònic dels pares o tutors.

En qualsevol cas, en la seva versió mòbil quan un usuari es descarrega l'aplicació, Dinantia sol·licita a l'usuari permís per accedir al calendari, la ubicació, el micròfon, el telèfon, l'emmagatzemament, i altres permisos (executar-se a l'inici, llegir alertes pendents, veure connexions de xarxa, impedir que el telèfon entri en modus suspensió, rebre dades d'internet, llegir la configuració dels serveis de Google, tenir accés complert a la xarxa, canviar configuració d'àudio etc.)

No està disponible al web la política de privacitat de l'aplicació i, pel que s'ha pogut comprovar, no es mostra tampoc en el moment d'instal·lar l'aplicació. Des de la pàgina web únicament es pot accedir a la política de privacitat i les condicions del tractament de les dades de la pròpia pàgina web. Per tant, es desconeix quines dades recull l'aplicació, la seva finalitat, quan de temps es guarden, si es comparteixen amb tercers, etc.

No s'ha trobat tampoc informació sobre la localització de l'emmagatzematge de les dades que gestiona l'aplicació, ni sobre les mesures de seguretat que implementa per protegir la informació emmagatzemada. Per exemple, no se sap quines mesures s'apliquen per garantir la confidencialitat de la informació emmagatzemada (si la informació és guarda en clar o encriptada, etc.), tampoc se sap quines mesures de seguretat s'apliquen per garantir la disponibilitat i la integritat de les dades (si hi es fan copies de seguretat de la informació que gestionen els centres educatius i la seva freqüència, etc.).

En relació amb les comunicacions no s'ha trobat informació sobre les mesures de seguretat que implementen (no se sap si les comunicacions estan xifrades o es fan en clar, no se sap si hi ha alguna mesura tècnica per verificar la identitat de qui fa la comunicació, etc.).

Pel que fa al desenvolupament de l'aplicació, no s'ha trobat tampoc cap informació (tecnologia utilitzada, dependències, etc.).

L'aplicació **ClassDojo**, és una aplicació web i mòbil que pertany a una empresa amb seu als Estats Units. D'acord al document de *"condicions de servei"* ofereix els serveis següents:

"*- Eines per ajudar els professors i els pares a comunicar-se entre ells.*
- Una forma pels professors per donar tasques i fer comentaris als estudiants, i altres eines per gestionar la classe.
- Una forma perquè els professors puguin compartir fotos, vídeos, arxius i altra informació de la classe amb els pares i els estudiants.
- Carpetes d'estudiant, amb les que els estudiants poden compartir la seva feina amb professors i pares.
- Activitats i altres continguts que professors o pares volen compartir amb els estudiants.
- Una forma per la direcció de l'escola per veure la comunitat escolar i comunicar-se amb els pares."

Aquesta aplicació pot ser utilitzada pels centres escolars pels diferents serveis que ofereix, tot i que també s'ofereix com una eina per als estudiants o els pares que, de forma particular, es donen d'alta com a eina d'aprenentatge. En el cas de la contractació dels serveis de la plataforma per part d'un centre escolar, és el propi centre qui es registra a l'aplicació i subscriu amb l'empresa proveïdora un contracte per a la prestació d'aquests serveis i l'alta a l'aplicació dels pares i dels alumnes la fa el propi centre, que pot enviar als pares un codi d'invitació. Tot i això, per poder emprar totes les funcionalitats, cal que els pares o tutors o fins i tot els alumnes es descarreguin l'aplicació al mòbil.

S'ha pogut comprovar que ClassDojo disposa d'una política de protecció de dades molt detallada (redactada en anglès) que es pot trobar a l'adreça https://www.ClassDojo.com/ca-es/privacy. En la qual es fa constar que compleix amb l'RGPD i altres regulacions de protecció de dades dels EEUU: COPPA (Children's Online Privacy Protection Act) i FERPA (Family Educational Rights and Privacy Act). El compliment amb les dos darreres ha estat certificada.

ClassDojo afirma recollir la següent informació en la seva aplicació, en funció dels serveis que presti:

• Nom i cognoms
• Número de telèfon
• Adreça electrònica
• Contrasenya
• ID del dispositiu mòbil
• Gènere
• Edat
• Informació sobre l'idioma
• Nom de l'escola
• Adreça de l'escola
• Número d'identificació local (districte escolar)
• Dades de geolocalització

• Fotografies, vídeos, documents, dibuixos i/o fitxers d'àudio
• Dades d'assistència a classe dels estudiants
• Punts de retroalimentació
• Adreça IP
• Detalls del navegador
• Temps d'accés
• Temps d'ús de l'aplicació
• Funcionalitats usades
• URL de d'origen
• Clics
• Temps d'activitat

Pel que fa a la seguretat de la informació, ClassDojo compta amb un document (https://www.ClassDojo.com/ca-es/security/) on detalla diferents aspectes de seguretat. Sense ànim d'exhaustivitat, els principals aspectes que recull son:

- Compliment de diferents estàndards de seguretat (ISO 27001, SOC 2, PCI DSS Level 1 i FISMA), que ha estat certificat per auditories externes. No es fa referència a l'ENS.

- Xifratge en repòs i en trànsit. Totes les comunicacions de dades són xifrades (protocol HTTPS). ClassDojo també afirma que xifra les dades personals identificables (en anglès, personally identificable information (PII)) a l'hora d'emmagatzemar-la. Ara bé, no queda clar si es refereix a tota la informació personal d'un usuari o només a informació com ara nom i cognoms, telèfon, adreça electrònica, etc.).

- Seguretat de les dades enfront dels treballadors de ClassDojo. Només es dona accés a les persones que per la seva feina ho necessiten (enginyers, científics de dades, gestors de producte i personal de suport). Es registra tot l'accés a la seva infraestructura i les contrasenyes per accedir són segures i amb autenticació multifactor.

- Confidencialitat de les dades. Busquen evitar que persones no autoritzades puguin tenir accés a les dades dels estudiants. (Procediments d'identificació i autenticació d'usuaris; Procediments de seguretat d'identificació/contrasenya; Xifratge de suports de dades arxivats; Comunicacions de dades xifrades).

- Integritat de les dades. Les mesures tècniques i organitzatives per controlar si s'han introduït, canviat o eliminat dades de l'alumne i per qui.

- Disponibilitat de la informació, ClassDojo compta amb mesures com còpies de seguretat distribuïdes geogràficament, redundància en mitjans tècnics pel processament de dades, etc.

El document també parla d'altres mesures de seguretat com ara les dedicades a garantir la seguretat física de les instal·lacions de processament de dades, el manteniment dels sistemes de tractament, etc.

En relació amb la conservació de les dades, ClassDojo especifica que si un compte resta inactiu durant 12 mesos, se suprimirà. Alguns continguts del compte d'estudiant es conservaran després de suprimir-lo per motius de compliment legal de l'escola (per exemple, el manteniment dels

"registres educatius" segons la Llei de privadesa i drets educatius de la família (FERPA)). El nom de l'estudiant proporcionat originalment pel professor es mantindrà, juntament amb qualsevol contingut enviat, com ara fotos i vídeos a Student Story.

En aquest dictamen, tal com es sol·licita a la consulta, ens centrarem en la utilització de les aplicacions objecte de la consulta únicament com a mecanisme per substituir l'agenda física en les llars d'infants municipals pel servei de comunicació que ofereixen, per bé que aquestes aplicacions com s'ha exposat tinguin moltes altres funcionalitats, algunes de les quals lligades amb l'aprenentatge, que no seran objecte d'aquest dictamen. En aquest sentit, es donarà resposta a les diferents qüestions plantejades en la consulta, tot i que s'alterarà l'ordre de les preguntes a efectes expositius.

III

Les escoles, i concretament en el cas plantejat en la consulta, les llars d'infants, en el desenvolupament de les seves activitats tracten dades personals de menors que requereixen una especial consideració per la situació de vulnerabilitat d'aquest col·lectiu i les conseqüències que es poden derivar d'un tractament inadequat de la seva informació. Per tant, cal extremar la diligència en el tractament d'aquesta informació.

En el cas concret de les comunicacions entre l'escola i els pares o tutors mitjançant un sistema de comunicació que ofereix serveis d'agenda, en el sentit de permetre a l'escola informar als pares o tutors sobre les activitats de l'aula o qüestions concretes relacionades amb el menor i la resposta dels pares o tutors a aquestes comunicacions (que poden incloure autoritzacions a la realització d'activitats), i que permet, així mateix, que els pares comuniquin al centre qüestions relacionades amb el menor com poden ser la justificació de no assistència per motius de salut, la necessitat de l'administració d'algun medicament, etc. comporta el tractament de dades personals tant dels pares o tutors de l'alumne, com dades dels mateixos alumnes que, en alguns casos, poden ser categories especials de dades.

Per tal de donar resposta a les preguntes formulades en la consulta cal tenir en consideració que tot tractament de dades ha de complir els principis i garanties del Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (en endavant, RGPD) i de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD).

L'RGPD articula la protecció de les dades personals a través del principi de responsabilitat proactiva segons el qual el responsable del tractament és responsable del compliment dels principis i garanties previstos a l'RGPD i, en concret, els recollits a l'apartat primer de l'article 5 RGPD: licitud, lleialtat i transparència (article 5.1.a), limitació de la finalitat (article 5.1.b), minimització de dades (article 5.1.c), exactitud (article 5.1.d), limitació del termini de conservació (article 5.1.e) i integritat i confidencialitat (article 5.1.f). D'acord amb aquest principi, el responsable del tractament ha de ser capaç de demostrar el seu compliment.

L'article 25 de l'RGPD regula la responsabilitat del responsable del tractament en els termes següents:

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento."

L'article 4.7 de l'RGPD defineix el responsable del tractament com " l*a persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento."*

Partint de la base que l'Escola (o si escau, l'Ajuntament) és la responsable del tractament de les dades personals necessàries per a l'exercici de les seves funcions ja siguin educatives i orientadores o altres relacionades amb les activitats pròpies del centre.

L'article 5.1.a) de l'RGPD estableix que tot tractament de dades personals ha de ser lícit, lleial i transparent en relació amb l'interessat (principi de licitud, lleialtat i transparència).

Per tal que un tractament sigui lícit cal comptar amb, al menys, una base jurídica de les previstes a l'article 6.1 de l'RGPD que legitimi aquest tractament, ja sigui el consentiment de la persona afectada, ja sigui alguna de les altres circumstàncies que preveu el mateix precepte. En l'àmbit de les administracions públiques, resulten d'especial interès, les bases jurídiques previstes en les lletres c) i e) de l'article 6.1 de l'RGPD, segons les quals el tractament serà lícit quan sigui necessari per al compliment d'una obligació legal aplicable al responsable del tractament (lletra c), o quan el tractament sigui necessari per al compliment d'un interès públic o en l'exercici de poders públics conferits al responsable del tractament (lletra e).

L'article 6.3 de l'RGPD estableix que les bases del tractament indicat a l'article 6.1. c) i e) han d'estar establertes pel Dret de la Unió europea o pel dret dels Estats membres que s'apliqui al responsable del tractament. La remissió a la base legítima establerta conforme el dret intern dels Estats membres a què fa referència aquest article requereix que la norma de desenvolupament, en tractar-se la protecció de dades personals d'un dret fonamental, tingui rang de llei (article 53 CE), tal com ha vingut a reconèixer l'article 8 de l'LOPDGDD.

Pel que fa al tractament de les dades personals dels alumnes, la disposició addicional vint-i-tresena de la Llei Orgànica 2/2006, de 3 de maig, d'Educació, estableix:

"Datos personales de los alumnos.

1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al

origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.

2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal.

En el caso de la cesión de datos entre Comunidades Autónomas o entre éstas y el Estado, las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas, en el seno de la Conferencia Sectorial de Educación."

Per tant, la LOE habilita als centres educatius, ja siguin de titularitat pública o privada, per al tractament de les dades personals del seu alumnat que siguin necessàries per a l'exercici de la seva funció educativa i orientadora.

L'apartat segon de la disposició de la LOE esmentada fa referència a la col·laboració dels pares, tutors i dels mateixos alumnes en l'obtenció d'aquesta informació. Per tant, en l'àmbit de la seva funció educativa i orientadora el centre està habilitat per a tractar les dades personals que siguin necessàries tant de l'alumne com dels pares o tutors. Fora d'aquests supòsits la base jurídica del tractament podrà ser el consentiment o una altra base de les previstes a l'article 6.1 RGPD, d'acord amb els requisits que s'estableixen a l'RGPD.

Escau també tenir en consideració la modificació introduïda a la LOE per la Llei orgànica 3/2020, de 29 de desembre, en concret la introducció d'un nou article 111 bis que estableix:

"1. El Ministerio de Educación y Formación Profesional establecerá, previa consulta a las Comunidades Autónomas, los estándares que garanticen la interoperabilidad entre los distintos sistemas de información utilizados en el Sistema Educativo Español, en el marco del Esquema Nacional de Interoperabilidad previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

(...)

“En el marco de la implantación de las citadas medidas, dentro de los sistemas de información propios de la gestión académica y administrativa se regulará un número identificativo para cada alumno o alumna, a fin de facilitar el intercambio de la información relevante, el seguimiento de las trayectorias educativas individualizadas, incluyendo las medidas educativas que en su caso se hubieran podido aplicar, y atender demandas de la estadística estatal e internacional y de las estrategias europeas para los sistemas de educación y formación. En cualquier caso, dicha regulación atenderá a la normativa relativa a la privacidad y protección de datos personales.

2. ***Los entornos virtuales de aprendizaje que se empleen en los centros docentes sostenidos con fondos públicos facilitarán la aplicación de planes educativos específicos diseñados por los docentes para la consecución de objetivos concretos del currículo, y deberán contribuir a la extensión del concepto de aula en el tiempo y en el espacio****. Por ello deberán, respetando los estándares de interoperabilidad, permitir a los alumnos y alumnas el acceso, desde cualquier sitio y en cualquier momento, a los entornos de aprendizaje disponibles en los centros docentes en los que estudien, con pleno respeto a lo dispuesto en la normativa aplicable en materia de propiedad intelectual, privacidad y protección de datos personales. Así mismo promoverán los principios de accesibilidad universal y diseño para todas las personas, tanto en formatos y contenidos como en herramientas y entornos virtuales de aprendizaje.*

3. El Ministerio de Educación y Formación Profesional impulsará, previa consulta a las Comunidades Autónomas, la compatibilidad de los formatos que puedan ser soportados por las herramientas y entornos virtuales de aprendizaje en el ámbito de los contenidos educativos digitales públicos, con el objeto de facilitar su uso con independencia de la plataforma tecnológica en la que se alberguen.
(...)

5. Las Administraciones educativas y los equipos directivos de los centros promoverán el uso de las tecnologías de la información y la comunicación (TIC) en el aula como medio didáctico apropiado y valioso para llevar a cabo las tareas de enseñanza y aprendizaje. Las Administraciones educativas deberán establecer las condiciones que hagan posible la eliminación en el ámbito escolar de las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red. Se fomentará la confianza y seguridad en el uso de las tecnologías prestando especial atención a la desaparición de estereotipos de género que dificultan la adquisición de competencias digitales en condiciones de igualdad.

6. El Ministerio de Educación y Formación Profesional elaborará y revisará, previa consulta a las Comunidades Autónomas, los marcos de referencia de la competencia digital que orienten la formación inicial y permanente del profesorado y faciliten el desarrollo de una cultura digital en los centros y en las aulas.

7. Las Administraciones públicas velarán por el acceso de todos los estudiantes a los recursos digitales necesarios, para garantizar el ejercicio del derecho a la educación de todos los niños y niñas en igualdad de condiciones.

En todo caso, las tecnologías de la información y la comunicación (TIC) y los recursos didácticos que se empleen, se ajustarán a la normativa reguladora de los servicios y sociedad de la información y de los derechos de propiedad intelectual, concienciando en el respeto de los derechos de terceros.

També en aquest sentit, l'article 83 de l'LOPDGDD estableix el següent:

"1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derecho fundamentales en Internet.

Així doncs, i tenint en compte aquest mandat de promoció de les competències digitals i la utilització d'entorns virtuals d'aprenentatge, es pot considerar que els tractaments de les dades dels alumnes amb aquesta finalitat tindria base jurídica en tractar-se d'una missió en interès públic (conforme l'article 6.1.e) de l'RGPD amb els requisits de la LOPDGDD i la LOE.

IV

Començant per la sisena pregunta que es planteja, cal determinar, en primer lloc, si el responsable del tractament de les dades que empren o emmagatzemen les aplicacions és l'escola o les empreses titulars d'aquestes aplicacions. Escau, doncs, analitzar la relació entre el centre escolar i l'empresa proveïdora de les aplicacions.

D'acord amb l'article 4.7 de l'RGPD el responsable del tractament és qui estableix el propòsit o el resultat del tractament (en aquest cas podria ser mantenir la comunicació amb les famílies amb finalitats educatives en temps de pandèmia); decideix sobre la finalitat i els usos de la informació; i decideix sobre els mitjans del tractament (en aquest cas els serveis oferts per una empresa externa que els proveeix d'una aplicació informàtica).

L'article 4.8 de l'RGPD defineix l'encarregat del tractament, com "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".*

La decisió sobre si el responsable del tractament és l'escola (la direcció de l'escola) o l'Ajuntament del qual depèn, és una qüestió organitzativa que caldrà determinar en funció de qui tingui realment, en el cas plantejat, la capacitat de decisió sobre els aspectes esmentats.

En qualsevol cas, l'empresa que presta el servei de plataformes accessibles a través d'Internet, en la mesura que tingui accés a les dades personals per prestar aquest servei, o les tracti de qualsevol altra manera (art. 4.2 RGPD), tindrà la consideració d'encarregada del tractament.

El responsable del tractament ha de triar un encarregat del tractament que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures tècniques i organitzatives apropiades, d'acord amb el que estableix l'RGPD, i que garanteixi la protecció dels drets de les persones afectades (article 28.1 RGPD). Per tant, hi ha un deure de diligència a l'hora d'escollir l' encarregat del tractament.

Aquest encàrrec s'ha de formalitzar mitjançant un contracte o un altre acte jurídic amb subjecció al dret de la Unió o dels estats membres que ha de regular els aspectes previstos a l'article 28.3 de l'RGPD:

" El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable."

Per tant, el responsable del tractament, per tal d'utilitzar aquestes aplicacions ha de subscriure un contracte o un altre document jurídic que vinculi a l'empresa titular d'aquestes aplicacions i que garanteixi que compleix els requeriments de l'RGPD i, en concret cadascun dels aspectes recollits a l'apartat tercer de l'article 28 del RGPD.

En el cas dels proveïdors d'aplicacions, com en el cas de l'aplicació ClassDojo, es freqüent que ofereixin clàusules generals d'acceptació del servei, que han de ser valorades pel responsable del tractament per determinar si permeten donar resposta a tots els requeriments i garanties a què fa referència l'article 28.3 de l'RGPD.

V

A la cinquena pregunta es planteja si és possible demanar el consentiment dels pares sense donar una altra alternativa a la comunicació amb l'escola. A aquest respecte s'ha de dir que, si la utilització de les aplicacions s'efectua en el context de comunicació amb els pares lligada a l'exercici de les funcions educatives i orientadores, la base jurídica d'aquest tractament podria ser, tal com s'ha exposat, l'article 6.1.e) de l'RGPD en relació amb la LOE.

No obstant això, res impedeix que l'escola pugui decidir utilitzar una determinada eina basant-se només en el consentiment, de manera que utilitzi una eina de comunicació només amb els pares que hi consentin. En aquest sentit, l'article 4.1 RGPD estableix que s'entén per consentiment "*toda manifestación libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen*".

D'entrada, i tal com recull el Dictamen 02/2013 del Grup de Treball de l'article 29 sobre les aplicacions dels dispositius intel·ligents, que analitza l'adequació a la normativa de protecció de dades el desenvolupament d'aplicacions en els dispositius i que recull recomanacions tant pels desenvolupadors com pels usuaris, cal diferenciar entre el consentiment previ a la instal·lació d'una aplicació, de la base jurídica del tractament de les dades personals. Tot i que aquest Dictamen és anterior a l'RGPD les consideracions que recull continuen vigents en molts aspectes. Així el punt 3.4.1 estableix:

"3.4.1 Consentimiento previo a la instalación y tratamiento de datos personales
En el caso de las aplicaciones, el principal fundamento jurídico aplicable es el consentimiento. Al instalar una aplicación, se introduce información en el dispositivo del usuario final. Muchas aplicaciones también acceden a los datos almacenados en el dispositivo, la lista de contactos, las fotografías, los vídeos y otra documentación personal. En todos estos casos, el artículo 5, apartado 3, de la Directiva sobre la privacidad electrónica exige el consentimiento del usuario tras habérsele facilitado información clara y completa, antes de la introducción y la extracción de datos del dispositivo.
Conviene observar la distinción entre el consentimiento requerido para introducir o leer información en el dispositivo y el consentimiento necesario para tener un fundamento jurídico para el tratamiento de los distintos tipos de datos personales."

En aquest cas cal distingir entre el consentiment que han de donar els pares o tutors per tal d' instal·lar en els seus dispositius l'aplicació, i el consentiment com a base jurídica per tractar les seves dades personals, que ha de reunir els requisits de l'RGPD i, per tant, ha de ser informat sobre tots els aspectes relacionats amb el tractament de les dades personals com a conseqüència de la utilització de l'aplicació per a la finalitat de comunicar-se amb el centre escolar.

Respecte del consentiment com a base jurídica en els tractaments de dades per part de les administracions públiques cal tenir en consideració que d'acord amb l'RGPD el consentiment no s'ha donat lliurement quan existeixi un desequilibri clar entre l'interessat i el responsable del tractament, així el considerant 42 RGPD posa de manifest que " *Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente"*.

Ara bé, això no vol dir que el consentiment no pugui ser una base legitima en els tractaments de dades que porti a terme una administració pública. Així, tal com recull el Grup de Treball de l'article 29 en les Directrius sobre el consentiment en el sentit del Reglament (UE) 2016/679, una escola pública pot sol·licitar el consentiment per a la publicació de les imatges dels seus alumnes en una revista de l'escola. Tal com conclou l'esmentat document, el consentiment en aquestes situacions seria una base jurídica vàlida sempre que *"no se negara a los alumnos la educación u otros servicios y ellos pudieran negarse al uso de dichas fotografías sin sufrir ningún perjuicio".*

En qualsevol cas, el consentiment ha de ser lliure. Per tant, es pot concloure que en general el consentiment únicament pot ser una base jurídica adequada si s'ofereix el control a l'interessat i aquest té una opció real d'acceptar o rebutjar els termes que se li ofereixen sense patir cap perjudici com a conseqüència de no donar el seu consentiment.

En conseqüència, si es vol fonamentar la utilització d'aquestes eines en el consentiment dels pares, i atès que la comunicació amb els pares es pot considerar que forma part necessàriament del contingut de la funció educativa i orientadora dels centres educatius, caldrà disposar d'alternatives per a poder seguir l'agenda i les comunicacions de l'escola, sense que això els comporti un perjudici.

VI

S'analitza a continuació la necessitat d'efectuar una avaluació d'impacte de la privacitat prèvia a la utilització d'aquestes aplicacions, en resposta a la pregunta número tres efectuada en la consulta. Qüestió aquesta que està estretament relacionada amb la pregunta quarta sobre quins són els principals riscos i quines mesures serien més adients per tal de minimitzar-los.

Amb independència que en qualsevol tractament de dades calgui fer una anàlisi dels riscos que comporta el tractament (considerant 76, *"El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo és alto")* l'apartat 1 de l'article 35 de l'RGPD estableix, amb caràcter general, l'obligació del responsable del tractament de dades de fer una avaluació d'impacte relativa a la protecció de dades (AIPD), amb caràcter previ a l'inici del tractament, quan sigui probable que per la seva naturalesa, abast, context o fins comportin un alt risc pels drets i llibertats de les persones físiques, alt risc que, segons el mateix RGPD, es veu incrementat quan els tractaments es realitzen utilitzant *"noves tecnologies".*

El mateix article 35.3 de l'RGPD concreta que, entre d'altres supòsits en què es derivi de les previsions de l'apartat primer, cal fer una avaluació d'impacte relativa a la protecció de dades en els següents supòsits:

"a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público."

El tractament de dades del cas que ens ocupa no sembla que es pugui encabir en cap dels supòsits referits.

Així, pel que fa al primer supòsit, no respon a una avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques basades en un tractament automatitzat, com l'elaboració de perfils.

Pel que fa al segon i tercer supòsit, per delimitar què cal entendre per *"tractament a gran escala"*, pot servir com a referència el document WP 243 *"Directrius sobre els delegats de protecció de dades (DPD)"* del Grup de Treball de l'article 29, en que considera que s'ha de tenir en compte el següent: el nombre d'interessats afectats, sigui en termes absoluts o com a proporció d'una determinada població, el volum i la varietat de dades tractades, la durada o permanència de l'activitat de tractament, l'extensió geogràfica de l'activitat de tractament. Així, i d'acord amb les directrius del GT29, en la mesura que la finalitat principal del tractament no és la comunicació de categories especials de dades i que el seu tractament es pot considerar ocasional, es pot

descartar en principi que existeixi en aquest cas un tractament a gran escala de categories especials de dades.

Cal tenir en compte també que l'article 35.4 de RGPD estableix que *"la autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1."* D'acord amb això, aquesta Autoritat, seguint les Directrius establertes pel Grup de Treball de l'article 29 en el document WP 248 esmentat, i els criteris per a la valoració del major risc previstos a l'article 28.2 de la LOPDGDD, ha elaborat i publicat al web de l'APDCAT una llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a la protecció de dades).

Així, en el moment d'analitzar els tractaments de dades serà necessari realitzar una avaluació de l'impacte relativa a la protecció de dades en la majoria dels casos en que aquest tractament compleixi amb dos o més criteris de la llista, llevat que el tractament es trobi en la llista de tractaments que no requereixen avaluació d'impacte a la qual es refereix l'article 35.5 del RGPD (fins al moment aquesta Autoritat no ha publicat cap llista amb exclusions als efectes de l'article 35.5).

Escau analitzar, doncs, si en el cas plantejat a la consulta es donen dos o més dels criteris de la llista. L'apartat 4 de la llista fa referència a: *"Tractaments que impliquin l'ús de categories especials de dades a què fa referència l'article 9.1 del RGPD"* . Cal tenir en consideració que els centres escolars poden tractar categories especials de dades dels menors, com dades de salut, origen racial, etc. en virtut de les funcions educatives i orientadores que els atribueix la LOE. Ara bé, cal tenir en compte que la inclusió d'aquest tipus d'informació en l'agenda o les comunicacions amb els pares sembla que només hauria de tenir un caràcter molt ocasional, en cap cas qualificable com a gran escala. Per tant, en principi si el tractament que es duu a terme només implica la recollida ocasional d'aquestes categories especials de dades necessàries per a les funcions educatives, no sembla que sigui exigible, per aquest fet, una avaluació d'impacte relativa a la protecció de dades, tenint en compte, a més, que es recollirien en compliment d'obligacions legals i que afectarien un nombre limitat de persones.

L'apartat 9 de la llista fa referència a "*Tractaments de dades de subjectes vulnerables o en risc d'exclusió social, incloent dades de menors de 14 anys, majors amb algun grau de discapacitat, discapacitats, persones que accedeixen a serveis socials i víctimes de violència de gènere, així com els seus descendents i persones que estiguin sota la seva guàrdia i custòdi*a" i l'aparat 10 a "*Tractaments que impliquin la utilització de noves tecnologies o un ús innovador de tecnologies consolidades, incloent la utilització de tecnologies a una nova escala, amb un nou objectiu o combinades amb altres, de manera que suposi noves formes de recollida i utilització de dades amb risc pels drets i llibertats de les persones*.". Ambdós criteris sembla que poden concórrer en el cas que ens ocupa.

Per tant, tot i que les categories especials de dades puguin tractar-se a l'aplicació només ocasionalment, el fet que afectin menors d'edat i que s'empri una tecnologia de la qual no es disposa d'inici de molta informació sobre el seu funcionament i els riscos que pot comportar, fan com a mínim recomanable, a la llum del principi de responsabilitat proactiva (art. 5.2 RGPD), fer una avaluació d'impacte relativa a la protecció de dades.

En aquest sentit, per fer l'avaluació d'impacte es recomana tenir en compte la Guia pràctica sobre l'AIPD, d'aquesta Autoritat, disponible al web www.apdcat.cat. Al web de l'Autoritat també hi podeu trobar i descarregar-vos una app per fer l'avaluació

Cal tenir en consideració, finalment que, si després d'haver fet la AIPD en resulta una situació d'alt risc que no s'ha pogut mitigar, s'ha de plantejar una consulta prèvia a l'Autoritat Catalana de Protecció de Dades, a la qual s'ha d'acompanyar una còpia de l'AIPD (art. 36 RGPD).

En qualsevol cas, i responent no només a la pregunta tercera sinó també a la pregunta quarta incloses a la consulta, serà a la vista d'aquesta avaluació d'impacte, que es podrà determinar quins son els riscos existents i quines mesures es poden adoptar per mitigar-los.

En qualsevol cas, caldrà prestar una especial atenció al fet que aquestes aplicacions poden utilitzar un model de "C*loud Computing*" o computació en el núvol. En el "*Cloud Computing*" les dades s'allotgen en el proveïdor de serveis en el núvol i s'accedeix als serveis a través d'Internet des de qualsevol dispositiu (telèfon mòbil, ordenador personal, tauleta). En aquest model els principals riscos derivats del tractament estan relacionats amb la correcta implantació de mesures de seguretat que evitin l'alteració, pèrdua, tractament o accés no autoritzat a les dades, a la implantació de mesures que garanteixin als titulars de les dades obtenir informació sobre el tractament i l'exercici dels drets i el control de les seves dades. Així mateix, en aquest model el proveïdor del servei pot estar en qualsevol lloc del mon, i per tant un dels principals riscos és que es produeixin transferències internacionals de dades dels menors, qüestió que s'analitza en el fonament de dret següent.

VII

Pel tal de respondre a la segona pregunta, relativa a les possibles transferències internacionals de dades que efectua una de les aplicacions, cal tenir en consideració que una transferència internacional de dades es produeix quan les dades personals tractades per un responsable o un encarregat del tractament en l'Espai Econòmic Europeu son enviats a un tercer país o organització internacional fora d'aquest territori.
L'RGPD recull el règim aplicable a les transferències internacionals als articles 44 a 49 que inclou la regulació dels mecanismes que permeten garantir que el lloc de destinació de les dades que s'han de transferir ofereix un nivell de protecció adequat en relació amb el que garanteix l'RGPD.

D'acord amb l'RGPD les dades només es poden comunicar fora de l'Espai Econòmic Europeu quan la Comissió Europea ha adoptat una decisió que reconeix a països, territoris o sectors específics (l'RGPD també hi inclou organitzacions internacionals) que ofereixen un nivell de protecció adequat (article 45 RGPD)

A manca d'una decisió d'adequació és possible efectuar transferències internacionals sense cap autorització expressa quan s'han ofert garanties adequades sobre la protecció que les dades rebran a la seva destinació, mitjançant un dels instruments previstos a l'article 46.2 RGPD:

"a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados

També és possible efectuar les transferències amb autorització d'una Autoritat de Control, en aquest cas l'APDCAT, en base a les garanties aportades mitjançant els instruments previstos a l'apartat 3 de l'article 46, següents:

"a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados."

Fora d'aquests supòsits l'article 49 RGPD estableix excepcions que permeten transferir les dades sense cap dels mecanismes anteriors quan es dona alguna de les circumstàncies que preveu, entre les quals que l'interessat hagi donat expressament el seu consentiment a la transferència proposada. Cal tenir en consideració però, que d'acord amb l'apartat 4 de l'article 49, s'exclou que la transferència es pugui basar en la possibilitat prevista a les lletres a), b) i c) relatives respectivament al consentiment de l'interessat, la transferència sigui necessària per a l'execució d'un contracte, o la celebració o execució d'un contracte en interès de l'interessat, respecte de les activitats que portin a terme les autoritats públiques en l'exercici dels seus poders públics.

Es a dir la transferència internacional no es pot basar en el consentiment dels interessats respecte de les activitats que portin a terme les autoritats públiques en l'exercici dels seus poders públics. Per tant, si l'ajuntament fonamenta el tractament en l'exercici de les seves funcions educatives i orientadores que li atribueix la LOE, la transferència internacional de les dades dels pares no es pot fonamentar en el seu consentiment.

Per a la transferència de dades a països que no garanteixen un nivell de protecció adequat, el responsable ha d'acreditar que l'encarregat del tractament està en disposició d'oferir garanties adequades. En tot cas, ha de garantir que els interessats compten amb drets exigibles i accions legals efectives.

En el cas que ens ocupa, l'aplicació ClassDojo realitza transferències de dades a Estats Units. Cal tenir en consideració que la Decisió d'execució 2016/1250 de la Comissió, de 12 de juliol de 2016, d'acord amb la Directiva 95/46/CE del Parlament Europeo i del Consell, sobre l'adequació de la protecció conferida per l'Escut de la privacitat UE-EE, ha estat invalidada per la Sentencia C-311/18 (Schrems II), del Tribunal de Justícia de la Unión Europea (TJUE) de 17 de juliol de 2020.

Per tant, a partir de l'esmentada Sentència no es poden efectuar transferències internacionals de dades a Estats Units sobre la base de l'Escut de Privacitat en haver estat invalidat pel TJUE, per considerar que Estats Units és un tercer país que no ofereix un nivell adequat de protecció.

A manca d'una decisió d'adequació, la recomanació del Comitè Europeu de Protecció de Dades de 10 de novembre de 2020 "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data",* recull eines per tal que els exportadors de dades puguin, en consonància amb el que es recull de la Sentencia del TJUE que invalida l'escut de privacitat, puguin garantir que el nivell de protecció en tercers països sigui *"essencialment equivalent"* al garantit a l'espai econòmic europeu.

En aquest context, respecte a la pregunta de la DPD: "*En el cas de clasdojo, que pensem que comporta transferències internacionals de dades, en el cas de voler continuar amb la seva utilització, cal demanar informe previ a l'APDCAT?* La resposta és que si no es disposa d'un dels mecanismes previstos a l'RGPD per proporcionar garanties adequades o no concorre alguna de les excepcions que sigui aplicable a les administracions públiques, no es podran efectuar aquestes transferències.

VIII

Finalment, a manera de conclusió i donant resposta a la primera pregunta de la consulta, cal determinar si la utilització de les aplicacions esmentades compleix la normativa de protecció de dades. Per a fer-ho, i a banda de les consideracions que ja s'han fet respecte els aspectes concrets comentats, cal fer esment d'algunes qüestions addicionals:

Tenint en compte l'àmbit concret en què es duria a terme el tractament, cal tenir en consideració que el Dictamen 02/2013, de 27 de febrer de 2013, sobre les aplicacions dels dispositius intel·ligents, del Grup de Treball de l'article 29 (GT29), recull entre les obligacions dels desenvolupadors d'aplicacions per donar compliment a la normativa de protecció de dades. Entre aquestes obligacions hi ha la de proporcionar una política de privacitat llegible, comprensible i fàcilment accessible que informi els consumidors, com a mínim sobre: qui és el responsable (identitat i dades de contacte); les categories de dades personals que recopilarà i tractarà l'aplicació; per a què es tractaran les dades; si les dades es comunicaran a tercers amb indicació concreta de a qui es comunicaran; els drets que tenen respecte a les seves dades personals, així com permetre l'exercici d'aquests drets i dels mecanismes per exercir-los; definir un període raonable de conservació de les dades recollides per l'aplicació i establir un període d'inactivitat passat el qual el compte es considera expirat. En definitiva el GT29 determina que aquesta informació hauria d'estar fàcilment accessible en la política de privacitat de l'aplicació, en conseqüència si manca algun d'aquests aspectes o quan la informació facilitada no ofereixi les garanties adequades, la recomanació congruent seria la de no utilitzar l'aplicació.

Respecte de l'aplicació Dinantia, pel que s'ha pogut comprovar, no es disposa d'informació publicada al seu web sobre la política de privacitat.

Pel que fa a l'aplicació ClassDojo, la política de privacitat que figura al seu web està redactada en anglès i no s'ha pogut comprovar que quan un usuari es descarrega l'aplicació tingui la informació concreta sobre la política de privacitat que s'aplica a les seves dades de manera accessible i entenedora.

El que si s'ha pogut comprovar és que en la política de privacitat publicada s'incorpora un document anomenat CLASSDOJO STUDENT DATA PRIVACY ADDENDUM, que té per objecte regular la relació contractual entre els centres escolars i l'empresa proveïdora de l'aplicació en relació amb el tractament de les dades personals dels estudiants.

Aquest document s'estructura en 7 punts o pactes, el setè dels quals regula les disposicions addicionals que apliquen als centres escolars ubicats a l'espai econòmic europeu i per tant els sigui d'aplicació l'RGPD, s'analitza a continuació aquesta addenda per als centres ubicats a l'espai de l'EEE.

L'apartat primer d'aquest pacte setè, sota el títol en anglès *"Roles"*, estableix que el centre escolar és el responsable del tractament i que designa a l'empresa proveïdora com a encarregada del tractament de les dades dels estudiants. Es valora positivament la transparència pel que fa a aquesta distribució de rols.

L'apartat segon sota el títol en anglès *"Scope"* indica l'abast de l'acord que diu que s'aplica al tractament de dades per part del proveïdor en nom del centre i d'acord amb les instruccions que aquest li doni en relació amb els serveis contractats. (remet a un annex B que recull la matèria, la finalitat del tractament i les dades i categories de dades de l'alumne).

S'ha pogut comprovar que existeix un annex A que descriu els serveis oferts i un annex B molt detallat que especifica totes les dades que es recullen, en aquest annex es remet a una pàgina web https://www.ClassDojo.com/transparency per obtenir informació sobre: les categories de dades que recopilen en funció dels diferents perfils d'usuari (estudiant, professor, pares, etc.) la naturalesa i finalitat de les activitats de tractament de les dades, el país on s'emmagatzemen les dades, la llista de categories especials de dades recopilades (s'indica que en aquest moment no es recullen). També s'indica una pàgina web amb la llista actual de proveïdors de serveis de l'empresa.

El punt tercer sota el títol en anglès *"Instructions"*, regula que el proveïdor únicament ha de tractar les dades de l'estudiant segons les instruccions documentades que li doni el centre i la prohibició de tractar les dades per a una altra finalitat diferent de les establertes. Es preveu que les instruccions són les fixades a l'acord tot i que el centre pot emetre instruccions addicionals si ho considera necessari per complir amb la normativa de protecció de dades, especifica quines són les persones autoritzades per donar instruccions (direcció del centre, delegat de protecció de dades o gerent del departament legal del centre). La possibilitat de donar instruccions amb relació al contractista, més enllà de les fixades a l'acord es valora positivament atès que és una de les funcions del responsable del tractament i ha de quedar per escrit en el contracte.

El punt quart sota el títol en anglès *"Subprocessing",* regula l'autorització del centre al proveïdor per a contractar als subencarregats del tractament que enumera en la llista de proveïdors del servei amb el compromís que recollirà les garanties suficients de tots els subencarregats d' implementar les mesures tècniques i organitzatives per complir la normativa de protecció de dades i els acords d'aquest document. No hi ha, però, una llista de les empreses subencarregades que permeti al responsable conèixer si n'hi ha i quines són. Respecte d'aquesta previsió és important que el centre tingui la capacitat d'oposar-se a determinades empreses actuïn com a subencarregades del tractament si consideren que no garanteixen suficientment el compliment de la normativa de protecció de dades.

El punt cinquè regula les transferències internacionals de dades, aquesta clàusula preveu que, el centre escolar autoritza al proveïdor a realitzar transferències internacionals de dades a països subjectes a una decisió d'adequació actual de la Comissió de la Unió Europea i a realitzar les transferències de dades enumerades a l'annex b. En concret, el proveïdor es compromet a mantenir una certificació a l'escut de privacitat. Aquest aspecte no es pot considerar actualment com a suficient, tenint en compte el que ja s'ha exposat en el fonament VII d'aquest dictamen.

El punt sisè sota el títol en anglès *"Personnel",* regula l'obligació del proveïdor d'implementar les mesures tècniques i organitzatives adequades per garantir que el personal tracta les dades d'acord amb les instruccions del responsable del tractament i remet als apartats de l'acord que regulen les obligacions, les contrasenyes d'accés i la capacitació dels empleats.

El punt setè sota el títol en anglès *"Confidentiality",* regula l'obligació del proveïdor de conservar les dades dels estudiants i qualsevol informació relacionada amb el tractament amb estricta confidencialitat.

El punt vuitè sota el títol en anglès *"Security and Personal Data Breaches"* estableix que el proveïdor té l'obligació d'implementar les mesures tècniques i organitzatives per garantir un nivell de seguretat apropiat als riscos que pugui oferir el tractament, inclòs el xifratge i la seudonimització de les dades de l'estudiant com s'estableix a l'apartat de l'acord corresponent a la seguretat de les dades. Un auditor extern certifica el compliment amb estàndards de seguretat com ara: ISO 27001, SOC 2, PCI DSS Level 1 i FISMA.

Cal tenir en compte però que l'ajuntament titular de les dades està sotmès al compliment de l'Esquema Nacional de Seguretat (ENS) d'acord amb el que preveu la disposició addicional primera de l'LOPDGDD. En el cas que s'analitza, tot i que ClassDojo compta en el seu web amb un document (https://www.ClassDojo.com/ca-es/security/) on detalla diferents aspectes de seguretat, tal com s'ha recollit al fonament jurídic II d'aquest dictamen, no s'ha pogut verificar que el proveïdor compleix amb totes les mesures de seguretat que es deriven de l'ENS.

Pel que fa a les violacions de seguretat estableix que el proveïdor ha d'informar el centre sense demora indeguda després de tenir coneixement d'una violació de seguretat de les dades i se sotmet al procediment establert a l'aparat de l'acord que regula els incompliments.

El punt novè sota el títol en anglès "*Assistance*" estableix que el proveïdor ha de proporcionar assistència raonable al centre escolar en el compliment de les obligacions de la normativa de protecció de dades respecte a: 1) el compliment de les sol·licituds per exercir els drets dels interessats, 2) respondre a consultes o queixes dels titulars de les dades 3) respondre a

investigacions i consultes de les autoritats de control, 4) notificar les violacions de dades personals de les dades dels estudiants del centre escolar, i 5) consultes prèvies amb Autoritats de control Recull el compromís del proveïdor d'informar el centre escolar si creu que una instrucció viola la normativa de protecció de dades. Es dóna compliment a les obligacions de garantir l'exercici dels drets dels interessats. No obstant això es troba a faltar una previsió sobre el sotmetiment a les auditories que determini el responsable o, com a mínim, el coneixement per part del responsable de les auditories independents a què se sotmeti la plataforma.

En aquest apartat es recull també una previsió en el sentit que, excepte que estigui prohibit per la UE o les lleis dels estats membres de la UE i subjecte a un procediment específic el proveïdor ha d'informar immediatament al centre escolar si rep una sol·licitud de les forces de l'ordre, els tribunals o qualsevol govern o qualsevol entitat, d'accedir a dades personals i, en qualsevol cas, es preveu expressament que si "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".

Tot i que el pacte quart de l'addenda de privacitat preveu que el proveïdor haurà d'eliminar totes les dades de l'estudiant quan ho sol·liciti el centre escolar, es troba a faltar la concreció respecte al destí que es donarà a les dades un cop finalitzat l'encàrrec del tractament en aquest pacte setè.

Per tant, es pot concloure que no es pot garantir que l'ús d'aquesta aplicació compleix la normativa de protecció de dades ateses les mancances analitzades relatives, entre d'altres, a disposar d'una política de privacitat fàcilment accessible i entenedora, a oferir garanties suficients pel que fa a les transferències internacionals de dades, a garantir el compliment de les mesures de seguretat de l'ENS o a què el responsable del tractament pugui oposar-se a la subcontractació de serveis a terceres empreses.

Conclusions

El centre educatiu o, si escau l'ajuntament del qual depengui la llar d'infants, és el responsable del tractament de les dades dels alumnes i dels pares, mentre que les empreses proveïdores de les aplicacions objecte de la consulta serien encarregats del tractament d'aquestes dades.

La utilització de les aplicacions per a la comunicació amb els pares lligada a l'exercici de les funcions educatives i orientadores, pot trobar cobertura a l'article 6.1.e) en relació amb les previsions de la LOE. En el cas que el tractament es vulgui basar en el consentiment, per tal que aquest sigui vàlid, els pares han de disposar d'alternatives per a poder seguir l'agenda i les comunicacions de l'escola, sense que això els comporti un perjudici.

Els principals riscos derivats de la utilització d'aquestes aplicacions estan relacionats amb la correcta implantació de mesures de seguretat que evitin l'alteració, pèrdua, tractament o accés no autoritzat a les dades, a la implantació de mesures que garanteixin als titulars de les dades obtenir informació sobre el tractament i l'exercici dels drets i el control de les seves dades, en especial els derivats de la utilització del cloud computing i la transferència internacional de dades. A aquests efectes i per identificar i si escau mitigar els riscos existents, resulta altament recomanable fer una avaluació d'impacte relativa a la protecció de dades.

Respecte a la consulta sobre si la utilització d'aquestes aplicacions compleix la normativa de protecció de dades cal tenir en consideració que el responsable del tractament ha de triar un encarregat del tractament que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures tècniques i organitzatives apropiades, d'acord amb el que estableix l'RGPD, i que garanteixi la protecció dels drets de les persones afectades.

Amb la informació facilitada i la que s'ha pogut obtenir d'Internet no es disposa de dades suficients per determinar si l'aplicació Dinantia ofereix les garanties necessàries que es requereix d'un encarregat del tractament.

Pel que fa a l'aplicació ClassDojo, tot i que la informació ofereix majors garanties d'adequació a l'RGPD que l'obtinguda en el cas de Dinantia, existeixen determinades mancances, concretades als fonaments jurídics VII i VIII d'aquest dictamen, que impedeixen concloure a partir de la informació disponible, l'adequació a l'RGPD.

Barcelona, 25 de febrer de 2021