CNS 3/2021

Dictamen en relación con la consulta formulada por un organismo en relación con diversas aplicaciones para comunicarse con las familias que están utilizando las guarderías municipales

Se presenta ante la Autoridad Catalana de Protección de Datos una consulta de la delegada de protección de datos (DPD) de varios ayuntamientos asistidos por la entidad en relación con diversas aplicaciones para comunicarse con las familias que están utilizando los hogares de niños municipales.

En la consulta se expone que para sustituir las comunicaciones de la agenda entre la guardería y los padres, debido a la situación sanitaria actual, algunos hogares han empezado a utilizar aplicaciones diversas, entre ellas dos aplicaciones (Dinantia y ClassDojo), de las que adjuntan los links:

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

También explica que algunos directores de los hogares han manifestado que disponían de la conformidad del inspector de enseñanza por su utilización y que también se están utilizando en varios colegios públicos de primaria.

En este contexto solicita el pronunciamiento de esta Autoridad sobre las siguientes cuestiones:

"1.¿La utilización de estas aplicaciones cumple la normativa de protección de datos?
2. En el caso de clasdojo, que pensamos que comporta transferencias internacionales de datos, en el caso de querer continuar con su utilización, ¿hay que pedir informe previo a la APDCAT?
3.¿Habría que realizar una evaluación de impacto, antes de la utilización de estas aplicaciones?
4.De poder continuar utilizando estas aplicaciones, ¿cuáles son los principales riesgos y qué medidas serían más adecuadas para minimizarlos?
5 De poder continuar utilizando estas aplicaciones, ya que se tiene el consentimiento de los padres, ¿es posible pedir el consentimiento sin dar otra alternativa a la comunicación con la escuela?

6.¿Quién es el responsable del tratamiento de los datos que almacena las app (la escuela o las empresas titulares de estas aplicaciones?")

A la vista de la consulta se ha pedido informe al área técnica de esta Autoridad para analizar las características técnicas de estas aplicaciones.

Analizada la consulta que no se acompaña de otra documentación, y teniendo en cuenta el informe del área técnica, de acuerdo con el informe de la Asesoría Jurídica emito el siguiente dictamen:

(...)

II

La consulta objeto de este dictamen hace referencia a la utilización por parte de determinadas guarderías municipales de dos aplicaciones para sustituir las comunicaciones de la agenda entre la guardería y los padres.

Para situar la consulta, es necesario describir, aunque sea brevemente, las dos aplicaciones citadas y su funcionamiento, en base a la información disponible en las respectivas páginas web: https://www.dinantia.com/es/ y https://www.ClassDojo.com/es-es/

La aplicación **Dinantia** se define como una aplicación para gestionar la comunicaciones en las escuelas: entre escuela y padres, y entre personal de la escuela, y ofrece las siguientes funcionalidades: *"publicación de notificaciones del centro y recordatorios, solicitud de autorizaciones con firma digital, formularios, control de asistencia, newsletter, control de lectura de las comunicaciones, denuncia de bullying".*

Esta aplicación se ofrece en versión para ordenador y móvil. Tal y como se hace constar en la web si un centro decide utilizar esta aplicación para comunicarse con los padres o tutores no es necesario que éstos se descarguen la aplicación en su móvil ya que las comunicaciones pueden llegar al correo electrónico de los padres o tutores .

En cualquier caso, en su versión móvil cuando un usuario se descarga la aplicación, Dinantia solicita al usuario permiso para acceder al calendario, ubicación, micrófono, teléfono, el almacenamiento, y otros permisos (ejecutarse al inicio, leer alertas pendientes, ver conexiones de red, impedir que el teléfono entre en modo suspensión, recibir datos de internet, leer la configuración de los servicios de Google, tener acceso completo en la red, cambiar configuración de audio etc.)

No está disponible en la web la política de privacidad de la aplicación y, por lo que se ha podido comprobar, no se muestra tampoco en el momento de instalar la aplicación. Desde la página web únicamente se puede acceder a la política de privacidad y condiciones del tratamiento de los datos de la propia página web. Por tanto, se desconoce qué datos recoge la aplicación, su finalidad, cuánto tiempo se guardan, si se comparten con terceros, etc.

Tampoco se ha encontrado información sobre la localización del almacenamiento de los datos que gestiona la aplicación, ni sobre las medidas de seguridad que implementa para proteger la información almacenada. Por ejemplo, no se sabe qué medidas se aplican para garantizar la confidencialidad de la información almacenada (si la información se guarda en claro o encriptada, etc.), tampoco se sabe qué medidas de seguridad se aplican para garantizar la disponibilidad y la integridad de los datos (si se realizan copias de seguridad de la información que gestionan los centros educativos y su frecuencia, etc.).

En relación con las comunicaciones no se ha encontrado información sobre las medidas de seguridad que implementan (no se sabe si las comunicaciones están cifradas o se hacen en claro, no se sabe si existe alguna medida técnica para verificar la identidad de quien hace la comunicación, etc.).

En cuanto al desarrollo de la aplicación, tampoco se ha encontrado ninguna información (tecnología utilizada, dependencias, etc.).

La aplicación **ClassDojo,** es una aplicación web y móvil que pertenece a una empresa con sede en Estados Unidos. De acuerdo al documento de *"condiciones de servicio"* ofrece los siguientes servicios:

"- Herramientas para ayudar a profesores y padres a comunicarse entre ellos.
- Una forma por los profesores para dar tareas y hacer comentarios a los estudiantes, y otras herramientas para gestionar la clase.
- Una forma para que los profesores puedan compartir fotos, vídeos, archivos y otra información de la clase con los padres y los estudiantes.
- Carpetas de estudiante, con las que los estudiantes pueden compartir su trabajo con profesores y padres.

- Actividades y otros contenidos que profesores o padres quieran compartir con los estudiantes.
- Una forma por la dirección de la escuela para ver a la comunidad escolar y comunicarse con los padres."

Esta aplicación puede ser utilizada por los centros escolares por los diferentes servicios que ofrece, aunque también se ofrece como una herramienta para los estudiantes o padres que, de forma particular, se dan de alta como herramienta de aprendizaje. En el caso de la contratación de los servicios de la plataforma por parte de un centro escolar, es el propio centro quien se registra en la aplicación y suscribe con la empresa proveedora un contrato para la prestación de estos servicios. alta en la aplicación de los padres y alumnos la hace el propio centro, que puede enviar a los padres un código de invitación. Sin embargo, para poder utilizar todas las funcionalidades, es necesario que los padres o tutores o incluso los alumnos se descarguen la aplicación en el móvil.

Se ha comprobado que ClassDojo dispone de una política de protección de datos muy detallada (redactada en inglés) que se puede encontrar en la dirección https://www.ClassDojo.com/ca-es/privacy. En la que se hace constar que cumple con el RGPD y otras regulaciones de protección de datos de EEUU: COPPA (Children's Online Privacy Protection Act) y FERPA (Family Educational Rights and Privacy Act). El cumplimiento con las dos últimas ha sido certificada.

ClassDojo afirma recoger la siguiente información en su aplicación, en función de los servicios que preste:

- Nombre y apellidos
- Número de teléfono
- Dirección electrónica
- Contraseña
- ID del dispositivo móvil
- Género
- Edad
- Información sobre el idioma
- Nombre de la escuela
- Dirección de la escuela
- Número de identificación local (distrito escolar)
- Datos de geolocalización

- Fotografías, vídeos, documentos, dibujos y/o archivos de audio
- Datos de asistencia a clase de los estudiantes
- Puntos de retroalimentación
- Dirección IP
- Detalles del navegador
- Tiempo de acceso
- Tiempo de uso de la aplicación
- Funcionalidades usadas
- URL de origen
- Clics
- Tiempo de actividad

En cuanto a la seguridad de la información, ClassDojo cuenta con un documento (https://www.ClassDojo.com/ca-es/security/) en el que detalla diferentes aspectos de seguridad. Sin ánimo de exhaustividad, los principales aspectos que recoge son:

- Cumplimiento de distintos estándares de seguridad (ISO 27001, SOC 2, PCI DSS Level 1 y FISMA), que ha sido certificado por auditorías externas. No se hace referencia al ENS.

- Cifrado en reposo y en tránsito. Todas las comunicaciones de datos son cifradas (protocolo HTTPS). ClassDojo también afirma que cifra los datos personales identificables (en inglés, personally identifiable information (PII)) a la hora de almacenarla. Ahora bien, no queda claro si se refiere a toda la información personal de un usuario o sólo a información como nombre y apellidos, teléfono, correo electrónico, etc.).

- Seguridad de los datos frente a los trabajadores de ClassDojo. Sólo se da acceso a las personas que por su trabajo lo necesitan (ingenieros, científicos de datos, gestores de producto y personal de soporte). Se registra todo el acceso a su infraestructura y sus contraseñas para acceder son seguras y con autenticación multifactor.

- Confidencialidad de los datos. Buscan evitar que personas no autorizadas puedan tener acceso a los datos de los estudiantes. (Procedimientos de identificación y autenticación de usuarios; Procedimientos de seguridad de identificación/contraseña; Cifrado de soportes de datos archivados; Comunicaciones de datos cifrados).

- Integridad de los datos. Las medidas técnicas y organizativas para controlar si se han introducido, cambiado o eliminado datos del alumno y por quién.

- Disponibilidad de la información, ClassDojo cuenta con medidas como copias de seguridad distribuidas geográficamente, redundancia en medios técnicos por el procesamiento de datos, etc.

El documento habla también de otras medidas de seguridad como las dedicadas a garantizar la seguridad física de las instalaciones de procesamiento de datos, el mantenimiento de los sistemas de tratamiento, etc.

En relación con la conservación de los datos, ClassDojo especifica que si una cuenta permanece inactiva durante 12 meses, se suprimirá. Algunos contenidos de la cuenta de estudiante se conservarán después de suprimirla por motivos de cumplimiento legal de la escuela (por ejemplo, el mantenimiento de los

"registros educativos" según la Ley de privacidad y derechos educativos de la familia (FERPA)). El nombre del estudiante proporcionado originalmente por el profesor se mantendrá, junto con cualquier contenido enviado, tales como fotos y vídeos en Student Story.

En este dictamen, tal y como se solicita en la consulta, nos centraremos en la utilización de las aplicaciones objeto de la consulta únicamente como mecanismo para sustituir la agenda física en las guarderías municipales por el servicio de comunicación que ofrecen, si bien estas aplicaciones como se ha expuesto tengan otras muchas funcionalidades, algunas de ellas ligadas con el aprendizaje, que no serán objeto de este dictamen. En este sentido, se dará respuesta a las distintas cuestiones planteadas en la consulta, aunque se alterará el orden de las preguntas a efectos expositivos.

III

Las escuelas, y concretamente en el caso planteado en la consulta, las guarderías, en el desarrollo de sus actividades tratan datos personales de menores que requieren una especial consideración por la situación de vulnerabilidad de este colectivo y las consecuencias que pueden derivarse de un tratamiento inadecuado de su información. Por tanto, es necesario extremar la diligencia en el tratamiento de esta información.

En el caso concreto de las comunicaciones entre la escuela y los padres o tutores mediante un sistema de comunicación que ofrece servicios de agenda, en el sentido de permitir a la escuela informar a los padres o tutores sobre las actividades del aula o cuestiones concretas relacionadas con el menor y la respuesta de los padres o tutores a estas comunicaciones (que pueden incluir autorizaciones a la realización de actividades), y que permite, asimismo, que los padres comuniquen al centro cuestiones relacionadas con el menor cómo pueden ser la justificación de no asistencia por motivos de salud, la necesidad de la administración de algún medicamento, etc. comporta el tratamiento de datos personales tanto de los padres o tutores del alumno, como datos de los propios alumnos que, en algunos casos, pueden ser categorías especiales de datos.

Para dar respuesta a las preguntas formuladas en la consulta es necesario tener en consideración que todo tratamiento de datos debe cumplir los principios y garantías del Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante, RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

El RGPD articula la protección de los datos personales a través del principio de responsabilidad proactiva según el cual el responsable del tratamiento es responsable del cumplimiento de los principios y garantías previstos en el RGPD y, en concreto, los recogidos en el apartado primero de el artículo 5 RGPD: licitud, lealtad y transparencia (artículo 5.1.a), limitación de la finalidad (artículo 5.1.b), minimización de datos (artículo 5.1.c), exactitud (artículo 5.1.d), limitación del plazo de conservación (artículo 5.1.e) e integridad y confidencialidad (artículo 5.1.f). De acuerdo con este principio, el responsable del tratamiento debe ser capaz de demostrar su cumplimiento.

El artículo 25 del RGPD regula la responsabilidad del responsable del tratamiento en los siguientes términos:

"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 se conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación a 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 oa 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."

"

El artículo 4.7 del RGPD define al responsable del tratamiento como *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento."*

Partiendo de la base de que la Escuela (o en su caso, el Ayuntamiento) es la responsable del tratamiento de los datos personales necesarios para el ejercicio de sus funciones ya sean educativas y orientadoras u otras relacionadas con las actividades propias del centro .

El artículo 5.1.a) del RGPD establece que todo tratamiento de datos personales debe ser lícito, leal y transparente en relación con el interesado (principio de licitud, lealtad y transparencia).

Para que un tratamiento sea lícito es necesario contar con, al menos, una base jurídica de las previstas en el artículo 6.1 del RGPD que legitime este tratamiento, ya sea el consentimiento de la persona afectada, ya sea alguna de las demás circunstancias que prevé el mismo precepto. En el ámbito de las administraciones públicas, resultan de especial interés, las bases jurídicas previstas en las letras c) ye) del artículo 6.1 del RGPD, según las cuales el tratamiento será lícito cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (letra c), o cuando el tratamiento sea necesario para el cumplimiento de un interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (letra e).

El artículo 6.3 del RGPD establece que las bases del tratamiento indicado en el artículo 6.1. c) ye) deben estar establecidas por el Derecho de la Unión europea o por el derecho de los Estados miembros que se aplique al responsable del tratamiento. La remisión a la base legítima establecida conforme al derecho interno de los Estados miembros a que se refiere este artículo requiere que la norma de desarrollo, al tratarse la protección de datos personales de un derecho fundamental, tenga rango de ley (artículo 53 CE), tal y como ha venido a reconocer el artículo 8 del LOPDDDD.

En cuanto al tratamiento de los datos personales de los alumnos, la disposición adicional vigésima tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, establece:

"Datos personales de los alumnos.

1. Los centros docentes podrán recabar las datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichas 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 tutoras y los propios alumnos tendrán que 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 sido 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 distintos del educativo sin consentimiento expreso.

3. En el tratamiento de las datos de los alumnos 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 las datos, incluidas las de carácter reservado, necesarias 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."

Por tanto, la LOE habilita a los centros educativos, ya sean de titularidad pública o privada, para el tratamiento de los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa y orientadora.

El apartado segundo de la disposición de la mencionada LOE hace referencia a la colaboración de los padres, tutores y de los propios alumnos en la obtención de esta información. Por tanto, en el ámbito de su función educativa y orientadora el centro está habilitado para tratar los datos personales que sean necesarios tanto del alumno como de los padres o tutores. Fuera de estos supuestos la base jurídica del tratamiento podrá ser el consentimiento u otra base de las previstas en el artículo 6.1 RGPD, de acuerdo con los requisitos que se establecen en el RGPD.

Es necesario también tener en consideración la modificación introducida en la LOE por la Ley orgánica 3/2020, de 29 de diciembre, en concreto la introducción de un nuevo artículo 111 bis que establece:

"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. Asimismo 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, a fin de facilitar su uso con independencia de la plataforma tecnológica en la que se albergan.
(...)

5. Las Administraciones educativas y equipos directivos de los centros promuevan 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 posibiliten 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 dificulten 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.

También en este sentido, el artículo 83 de la LOPDDDD establece lo siguiente:

"1. El sistema educativo garantizará la plena inserción de los alumnos 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 derechos fundamentales en Internet.

Así pues, y teniendo en cuenta este mandato de promoción de las competencias digitales y la utilización de entornos virtuales de aprendizaje, se puede considerar que los tratamientos de los datos de los alumnos a tal fin tendría base jurídica al tratarse de una misión en interés público (conforme el artículo 6.1.e) del RGPD con los requisitos de la LOPDGDD y la LOE.

IV

Empezando por la sexta pregunta que se plantea, es necesario determinar, en primer lugar, si el responsable del tratamiento de los datos que emplean o almacenan las aplicaciones es la escuela o las empresas titulares de estas aplicaciones. Es necesario, pues, analizar la relación entre el centro escolar y la empresa proveedora de las aplicaciones.

De acuerdo con el artículo 4.7 del RGPD, el responsable del tratamiento es quien establece el propósito o el resultado del tratamiento (en este caso podría ser mantener la comunicación con las familias con fines educativos en tiempo de pandemia); decide sobre la finalidad y los usos de la información; y decide sobre los medios del tratamiento (en este caso los servicios ofrecidos por una empresa externa que les provee de una aplicación informática).

El artículo 4.8 del RGPD define el encargado del tratamiento, como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".*

La decisión sobre si el responsable del tratamiento es la escuela (cuya dirección de la escuela) o el Ayuntamiento del que depende, es una cuestión organizativa que habrá que determinar en función de quien tenga realmente, en el caso planteado, la capacidad de decisión sobre los aspectos citados.

En cualquier caso, la empresa que presta el servicio de plataformas accesibles a través de Internet, en la medida en que tenga acceso a los datos personales para prestar este servicio, o los trate de cualquier otra forma (art. 4.2 RGPD), tendrá la consideración de encargada del tratamiento.

El responsable del tratamiento elegirá un encargado del tratamiento que ofrezca garantías suficientes respecto de la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas (artículo 28.1 RGPD). Por tanto, hay un deber de diligencia a la hora de escoger el encargado del tratamiento.

Este encargo debe formalizarse mediante un contrato u otro acto jurídico con sujeción al derecho de la Unión o de los Estados miembros que debe regular los aspectos previstos en el artículo 28.3 del 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 las datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive 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 en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste 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 todas las 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 las 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."

Por tanto, el responsable del tratamiento, con el fin de utilizar estas aplicaciones debe suscribir un contrato u otro documento jurídico que vincule a la empresa titular de estas aplicaciones y que garantice que cumple los requerimientos del RGPD y, en concreto cada uno de los aspectos recogidos en el apartado tercero del artículo 28 del RGPD.

En el caso de los proveedores de aplicaciones, como en el caso de la aplicación ClassDojo, es frecuente que ofrezcan cláusulas generales de aceptación del servicio, que deben ser valoradas por el responsable del tratamiento para determinar si permiten dar respuesta a todos los requerimientos y garantías a que se refiere el artículo 28.3 del RGPD.

V

En la quinta pregunta se plantea si es posible pedir el consentimiento de los padres sin dar otra alternativa a la comunicación con la escuela. A este respecto debe decirse que, si la utilización de las aplicaciones se efectúa en el contexto de comunicación con los padres ligada al ejercicio de las funciones educativas y orientadoras, la base jurídica de este tratamiento podría ser tal como se ha expuesto, el artículo 6.1.e) del RGPD en relación con la LOE.

Sin embargo, nada impide que la escuela pueda decidir utilizar una determinada herramienta basándose sólo en el consentimiento, de modo que utilice una herramienta de comunicación sólo con los padres que consienten. En este sentido, el artículo 4.1 RGPD establece que se entiende por consentimiento *"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 las datos personales que le conciernen".*

De entrada, y tal y como recoge el Dictamen 02/2013 del Grupo de Trabajo del artículo 29 sobre las aplicaciones de los dispositivos inteligentes, que analiza la adecuación a la normativa de protección de datos el desarrollo de aplicaciones en los dispositivos y que recoge recomendaciones tanto para los desarrolladores como para los usuarios, es necesario diferenciar entre el consentimiento previo a la instalación de una aplicación, de la base jurídica del tratamiento de los datos personales. Aunque este Dictamen es anterior al RGPD las consideraciones que recoge siguen vigentes en muchos aspectos. Así, el punto 3.4.1 establece:

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 introduzca información en el dispositivo del usuario final. Muchas aplicaciones también acceden a las datos almacenadas 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 haberle facilitado información clara y completa, antes de la introducción y 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 este caso hay que distinguir entre el consentimiento que deben dar los padres o tutores para instalar en sus dispositivos la aplicación, y el consentimiento como base jurídica para tratar sus datos personales, que debe reunir los requisitos del RGPD y, por tanto, debe ser informado sobre todos los aspectos relacionados con el tratamiento de sus datos personales como consecuencia de la utilización de la aplicación para la finalidad de comunicarse con el centro escolar.

Respecto al consentimiento como base jurídica en los tratamientos de datos por parte de las administraciones públicas hay que tener en consideración que de acuerdo con el RGPD el consentimiento no se ha dado libremente cuando exista un desequilibrio claro entre el interesado y el responsable del tratamiento, así el considerando 42 RGPD pone de manifiesto que *"Para garantizar que el consentimiento se haya dado libremente, éste no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por tanto improbable que el consentimiento se haya dado libremente".*

Sin embargo, esto no quiere decir que el consentimiento no pueda ser una base legitima en los tratamientos de datos que lleve a cabo una administración pública. Así, tal y como recoge el Grupo de Trabajo del artículo 29 en las Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, una escuela pública puede solicitar el consentimiento para la publicación de las imágenes de sus alumnos en una revista de la escuela. Tal y como concluye el citado documento, el consentimiento en estas situaciones sería una base jurídica válida siempre que *"no se negara a los alumnos la educación u otros servicios y ellos pudieran negarse al uso de dichas fotografías sin sufrir ningún perjuc*

En cualquier caso, el consentimiento debe ser libre. Por tanto, se puede concluir que en general el consentimiento únicamente puede ser una base jurídica adecuada si se ofrece el control al interesado y éste tiene una opción real de aceptar o rechazar los términos que se le ofrecen sin sufrir ningún perjuicio como a consecuencia de no dar su consentimiento.

En consecuencia, si se quiere fundamentar la utilización de estas herramientas en el consentimiento de los padres, y dado que la comunicación con los padres puede considerarse que forma parte necesariamente del contenido de la función educativa y orientadora de los centros educativos, habrá que disponer de alternativas para poder seguir la agenda y las comunicaciones de la escuela, sin que esto les comporte un perjuicio.

VI

Se analiza a continuación la necesidad de efectuar una evaluación de impacto de la privacidad previa a la utilización de estas aplicaciones, en respuesta a la pregunta número tres efectuada en la consulta. Cuestión esta que está estrechamente relacionada con la pregunta cuarta sobre cuáles son los principales riesgos y qué medidas serían más adecuadas para minimizarlos.

Con independencia de que en cualquier tratamiento de datos sea necesario realizar un análisis de los riesgos que comporta el tratamiento (considerante 76, *"El riesgo debe ponderarse en base a una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto")* el apartado 1 del artículo 35 del RGPD establece, con carácter general, la obligación del responsable del tratamiento de datos de realizar una evaluación de impacto relativa a la protección de datos (AIPD), con carácter previo al inicio del tratamiento, cuando sea probable que por su naturaleza, alcance, contexto o fines comporten un alto riesgo por los derechos y libertades de las personas físicas, alto riesgo que, según el propio RGPD, se ve incrementado cuando los tratamientos se realizan utilizando *nuevas tecnologías.*

El mismo artículo 35.3 del RGPD concreta que, entre otros supuestos en que se derive de las previsiones del apartado primero, es necesario realizar una evaluación de impacto relativa a la protección de datos en los siguientes supuestos:

> *"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 las datos personales relativas 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 tratamiento de datos del caso que nos ocupa no parece que pueda incluirse en ninguno de los supuestos referidos.

Así, en lo que se refiere al primer supuesto, no responde a una evaluación sistemática y exhaustiva de aspectos personales de personas físicas basadas en un tratamiento automatizado, como la elaboración de perfiles.

En cuanto al segundo y tercer supuesto, para delimitar qué debe entenderse por *"tratamiento a gran escala",* puede servir como referencia el documento WP 243 *"Directrices sobre los delegados de protección de datos (DPD)"* del Grupo de Trabajo del artículo 29, en que considera que debe tenerse en cuenta lo siguiente: el número de interesados afectados, sea en términos absolutos o como proporción de una determinada población, el volumen y la variedad de datos tratados, la duración o permanencia de la actividad de tratamiento, la extensión geográfica de la actividad de tratamiento. Así, y de acuerdo con las directrices del GT29, en la medida en que la finalidad principal del tratamiento no es la comunicación de categorías especiales de datos y que su tratamiento puede considerarse ocasional, se puede

descartar primeramente que exista en este caso un tratamiento a gran escala de categorías especiales de datos.

Hay que tener en cuenta también que el artículo 35.4 de RGPD establece 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. "*
De acuerdo con ello, esta Autoridad, siguiendo las Directrices establecidas por el Grupo de Trabajo del artículo 29 en el mencionado documento WP 248, y los criterios para la valoración del mayor riesgo previstos en el artículo 28.2 de la LOPDGDD, ha elaborado y publicado en la web de la APDCAT una lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos).

Así, en el momento de analizar los tratamientos de datos será necesario realizar una evaluación del impacto relativa a la protección de datos en la mayoría de los casos en que este tratamiento cumpla con dos o más criterios de la lista, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren evaluación de impacto a la que se refiere el artículo 35.5 del RGPD (hasta el momento esta Autoridad no ha publicado ninguna lista con exclusiones a efectos del artículo 35.5).

Es necesario analizar, pues, si en el caso planteado en la consulta se dan dos o más de los criterios de la lista. El apartado 4 de la lista hace referencia a: *"Tratamientos que impliquen el uso de categorías especiales de datos a que se refiere el artículo 9.1 del RGPD" .* Es necesario tener en consideración que los centros escolares pueden tratar categorías especiales de datos de los menores, como datos de salud, origen racial, etc. en virtud de las funciones educativas y orientadoras que les atribuye la LOE. Ahora bien, debe tenerse en cuenta que la inclusión de este tipo de información en la agenda o las comunicaciones con los padres parece que sólo debería tener un carácter muy ocasional, en ningún caso calificable como gran escala. Por tanto, en principio si el tratamiento que se lleva a cabo sólo implica la recogida ocasional de estas categorías especiales de datos necesarias para las funciones educativas, no parece que sea exigible, por este hecho, una evaluación de impacto relativa a la protección de datos, teniendo en cuenta, además, que se recogerían en cumplimiento de obligaciones legales y que afectarían a un número limitado de personas.

El apartado 9 de la lista hace referencia a *"Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia"* y el aparato 10 a *"Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo por los derechos y libertades de las personas.".* Ambos criterios parece que pueden concurrir en caso de que nos ocupa.

Por tanto, aunque las categorías especiales de datos puedan tratarse en la aplicación sólo ocasionalmente, el hecho de que afecten a menores de edad y que se utilice una tecnología de la que no se dispone de inicio de mucha información sobre su funcionamiento y los riesgos que puede comportar, hacen como mínimo recomendable, a la luz del principio de responsabilidad proactiva (art. 5.2 RGPD), realizar una evaluación de impacto relativa a la protección de datos.

En este sentido, para realizar la evaluación de impacto se recomienda tener en cuenta la Guía práctica sobre la AIPD, de esta Autoridad, disponible en la web www.apdcat.cat. En la web de la Autoridad también puede encontrar y descargarse una app para hacer la evaluación

Hay que tener en consideración, finalmente que, si después de haber realizado la AIPD resulta una situación de alto riesgo que no se ha podido mitigar, debe plantearse una consulta previa a la Autoridad Catalana de Protección de Datos, a la que debe acompañarse una copia de la AIPD (art. 36 RGPD).

En cualquier caso, y respondiendo no sólo a la pregunta tercera sino también a la pregunta cuarta incluidas en la consulta, será a la vista de esta evaluación de impacto, que podrá determinar cuáles son los riesgos existentes y qué medidas se pueden adoptar para mitigarlos.

En cualquier caso, habrá que prestar especial atención a que estas aplicaciones pueden utilizar un modelo de *"Cloud Computing"* o computación en la nube. En el *"Cloud Computing"* los datos se alojan en el proveedor de servicios en la nube y se accede a los servicios a través de Internet desde cualquier dispositivo (teléfono móvil, ordenador personal, tableta). En este modelo, los principales riesgos derivados del tratamiento están relacionados con la correcta implantación de medidas de seguridad que eviten la alteración, pérdida, tratamiento o acceso no autorizado a los datos, a la implantación de medidas que garanticen a los titulares de los datos obtener información sobre el tratamiento y el ejercicio de los derechos y el control de sus datos. Asimismo, en este modelo el proveedor del servicio puede estar en cualquier lugar del mundo, y por tanto uno de los principales riesgos es que se produzcan transferencias internacionales de datos de los menores, cuestión que se analiza en el fundamento de derecho siguiente.

VII

Con el fin de responder a la segunda pregunta, relativa a las posibles transferencias internacionales de datos que efectúa una de las aplicaciones, es necesario tener en consideración que una transferencia internacional de datos se produce cuando los datos personales tratados por un responsable o un encargado del tratamiento en el Espacio Económico Europeo son enviados a un tercer país u organización internacional fuera de ese territorio.
El RGPD recoge el régimen aplicable a las transferencias internacionales a los artículos 44 a 49 que incluye la regulación de los mecanismos que permiten garantizar que el lugar de destino de los datos a transferir ofrece un nivel de protección adecuado en relación con lo que garantiza el RGPD.

De acuerdo con el RGPD los datos sólo pueden comunicarse fuera del Espacio Económico Europeo cuando la Comisión Europea ha adoptado una decisión que reconoce a países, territorios o sectores específicos (el RGPD también incluye organizaciones internacionales) que ofrecen un nivel de protección adecuado (artículo 45 RGPD)

A falta de una decisión de adecuación es posible efectuar transferencias internacionales sin autorización expresa alguna cuando se han ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino, mediante uno de los instrumentos previstos en el artículo 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 conforme al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado conforme 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 las relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado conforme 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 las relativas a los derechos de los interesados

También es posible efectuar las transferencias con autorización de una Autoridad de Control, en este caso el APDCAT, en base a las garantías aportadas mediante los instrumentos previstos en el apartado 3 del artículo 46, siguientes:

a) cláusulas contractuales entre el responsable u encargado y responsable, encargado o destinatario de las 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."

Fuera de estos supuestos el artículo 49 RGPD establece excepciones que permiten transferir los datos sin ninguno de los mecanismos anteriores cuando se da alguna de las circunstancias previstas, entre las que el interesado haya dado expresamente su consentimiento a la transferencia propuesta. Sin embargo, hay que tener en consideración que, de acuerdo con el apartado 4 del artículo 49, se excluye que la transferencia se pueda basar en la posibilidad prevista en las letras a), b) yc) relativas respectivamente al consentimiento de interesado, la transferencia sea necesaria para la ejecución de un contrato, o la celebración o ejecución de un contrato en interés del interesado, respecto de las actividades que lleven a cabo las autoridades públicas en el ejercicio de los suyos poderes públicos.

Es decir, la transferencia internacional no puede basarse en el consentimiento de los interesados respecto de las actividades que lleven a cabo las autoridades públicas en el ejercicio de sus poderes públicos. Por tanto, si el ayuntamiento fundamenta el tratamiento en el ejercicio de sus funciones educativas y orientadoras que le atribuye la LOE, la transferencia internacional de los datos de los padres no puede fundamentarse en su consentimiento.

Para la transferencia de datos a países que no garantizan un nivel de protección adecuado, el responsable debe acreditar que el encargado del tratamiento está en disposición de ofrecer garantías adecuadas. En todo caso, debe garantizar que los interesados cuenten con derechos exigibles y acciones legales efectivas.

En caso de que nos ocupa, la aplicación ClassDojo realiza transferencias de datos a Estados Unidos. Hay que tener en consideración que la Decisión de ejecución 2016/1250 de la Comisión, de 12 de julio de 2016, de acuerdo con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE, ha sido invalidada por la Sentencia C-311/18 (Schrems II), del Tribunal de Justicia de la Unión Europea (TJUE) de 17 de julio de 2020.

Por tanto, a partir de la citada Sentencia no se pueden efectuar transferencias internacionales de datos a Estados Unidos sobre la base del Escudo de Privacidad al haber sido invalidado por el TJUE, por considerar que Estados Unidos es un tercer país que no ofrece un nivel adecuado de protección.

A falta de una decisión de adecuación, la recomendación del Comité Europeo de Protección de Datos de 10 de noviembre de 2020 *"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"*, recoge herramientas para que los exportadores de datos puedan, en consonancia con lo que se recoge de la Sentencia del TJUE que invalida el escudo de privacidad, puedan garantizar que el nivel de protección en terceros países sea *"esencialmente equivalente"* al garantizado en espacio económico europeo.

En este contexto, respecto a la pregunta de la DPD: *"En el caso de clasdojo, ¿que pensamos que comporta transferencias internacionales de datos, en el caso de querer continuar con su utilización, es necesario pedir informe previo a la APDCAT?* La respuesta es que si no se dispone de uno de los mecanismos previstos en el RGPD para proporcionar garantías adecuadas o no concurre alguna de las excepciones que sea de aplicación a las administraciones públicas, no se podrán efectuar estas transferencias.

VIII

Finalmente, a modo de conclusión y dando respuesta a la primera pregunta de la consulta, es necesario determinar si la utilización de las mencionadas aplicaciones cumple la normativa de protección de datos. Para ello, y aparte de las consideraciones que ya se han hecho respecto a los aspectos concretos comentados, hay que mencionar algunas cuestiones adicionales:

Teniendo en cuenta el ámbito concreto en el que se llevaría a cabo el tratamiento, es necesario tener en consideración que el Dictamen 02/2013, de 27 de febrero de 2013, sobre las aplicaciones de los dispositivos inteligentes, del Grupo de Trabajo del artículo 29 (GT29), recoge entre las obligaciones de los desarrolladores de aplicaciones para dar cumplimiento a la normativa de protección de datos. Entre estas obligaciones está la de proporcionar una política de privacidad legible, comprensible y fácilmente accesible que informe a los consumidores, al menos sobre: quién es el responsable (identidad y datos de contacto); las categorías de datos personales que recopilará y tratará la aplicación; para qué se tratarán los datos; si los datos se comunicarán a terceros con indicación concreta de a quiénes se comunicarán; los derechos que tienen respecto a sus datos personales, así cómo permitir el ejercicio de estos derechos y de los mecanismos para ejercerlos; definir un período razonable de conservación de los datos recogidos por la aplicación y establecer un período de inactividad pasado el cual la cuenta se considera expirada. En definitiva, el GT29 determina que esta información debería estar fácilmente accesible en la política de privacidad de la aplicación, en consecuencia si falta alguno de estos aspectos o cuando la información facilitada no ofrezca las garantías adecuadas, la recomendación congruente sería la de no utilizar la aplicación.

Respecto a la aplicación Dinantia, por lo que se ha podido comprobar, no se dispone de información publicada en su web sobre la política de privacidad.

En cuanto a la aplicación ClassDojo, la política de privacidad que figura en su web está redactada en inglés y no se ha podido comprobar que cuando un usuario se descarga la aplicación tenga la información concreta sobre la política de privacidad que se aplica a sus datos de forma accesible y entendedora.

Lo que si se ha podido comprobar es que en la política de privacidad publicada se incorpora un documento llamado CLASSDOJO STUDENT FECHA PRIVACY ADDENDUM, que tiene por objeto regular la relación contractual entre los centros escolares y la empresa proveedora de la aplicación en relación con el tratamiento de los datos personales de los estudiantes.

Este documento se estructura en 7 puntos o pactos, cuyo séptimo regula las disposiciones adicionales que aplican a los centros escolares ubicados en el espacio económico europeo y por tanto les sea de aplicación el RGPD, se analiza a continuación esta adenda para los centros ubicados en el espacio del EEE.

El apartado primero de este pacto séptimo, bajo el título en inglés *"Roles",* establece que el centro escolar es el responsable del tratamiento y que designa a la empresa proveedora como encargada del tratamiento de los datos de los estudiantes. Se valora positivamente la transparencia en lo que respecta a esta distribución de roles.

El apartado segundo bajo el título en inglés *"Scope"* indica el alcance del acuerdo que dice que se aplica al tratamiento de datos por parte del proveedor en nombre del centro y de acuerdo con las instrucciones que éste le dé en relación con los servicios contratados. (remite a un anexo B que recoge la materia, la finalidad del tratamiento y los datos y categorías de datos del alumno).

Se ha podido comprobar que existe un Anexo A que describe los servicios ofrecidos y un Anexo B muy detallado que especifica todos los datos que se recogen, en este Anexo se remite a una página web https://www.ClassDojo.com/transparency para obtener información sobre: las categorías de datos que recopilan en función de los diferentes perfiles de usuario (estudiante, profesor, padres, etc.) la naturaleza y finalidad de las actividades de tratamiento de los datos, el país en el que se almacenan los datos , la lista de categorías especiales de datos recopiladas (se indica que en este momento no se recogen). También se indica una página web con la lista actual de proveedores de servicios de la empresa.

El punto tercero bajo el título en inglés *"Instructions",* regula que el proveedor únicamente debe tratar los datos del estudiante según las instrucciones documentadas que le dé el centro y la prohibición de tratar los datos para otra finalidad distinta de las establecidas. Se prevé que las instrucciones son las fijadas en el acuerdo aunque el centro puede emitir instrucciones adicionales si lo considera necesario para cumplir con la normativa de protección de datos, especifica cuáles son las personas autorizadas para dar instrucciones (dirección del centro, delegado de protección de datos o gerente del departamento legal del centro). La posibilidad de dar instrucciones en relación con el contratista, más allá de las fijadas en el acuerdo se valora positivamente dado que es una de las funciones del responsable del tratamiento y debe quedar por escrito en el contrato.

El punto cuarto bajo el título en inglés *"Subprocessing",* regula la autorización del centro al proveedor para contratar a los subencargados del tratamiento que enumera en la lista de proveedores del servicio con el compromiso de que recogerá las garantías suficientes de todos los subencargados de implementar las medidas técnicas y organizativas para cumplir con la normativa de protección de datos y los acuerdos de este documento. Sin embargo, no hay una lista de las empresas subencargadas que permita al responsable conocer si hay y cuáles son. Respecto a esta previsión es importante que el centro tenga la capacidad de oponerse a determinadas empresas actúen como subencargadas del tratamiento si consideran que no garantizan suficientemente el cumplimiento de la normativa de protección de datos.

El punto quinto regula las transferencias internacionales de datos, esta cláusula prevé que, el centro escolar autoriza al proveedor a realizar transferencias internacionales de datos a países sujetos a una decisión de adecuación actual de la Comisión de la Unión Europea ya realizar las transferencias de datos enumeradas en el anexo b. En concreto, el proveedor se compromete a mantener una certificación en el escudo de privacidad. Este aspecto no puede considerarse actualmente como suficiente, teniendo en cuenta lo ya expuesto en el fundamento VII de este dictamen.

El punto sexto bajo el título en inglés *"Personnel",* regula la obligación del proveedor de implementar las medidas técnicas y organizativas adecuadas para garantizar que el personal trata los datos de acuerdo con las instrucciones del responsable del tratamiento y remite a los apartados de el acuerdo que regulan las obligaciones, contraseñas de acceso y capacitación de los empleados.

El punto séptimo bajo el título en inglés *"Confidentiality",* regula la obligación del proveedor de conservar los datos de los estudiantes y cualquier información relacionada con el tratamiento con estricta confidencialidad.

El punto octavo bajo el título en inglés *"Security and Personal Data Breaches"* establece que el proveedor tiene la obligación de implementar las medidas técnicas y organizativas para garantizar un nivel de seguridad apropiado a los riesgos que pueda ofrecer el tratamiento, incluido el cifrado y la seudonimización de los datos del estudiante como se establece en el apartado del acuerdo correspondiente a la seguridad de los datos. Un auditor externo certifica el cumplimiento con estándares de seguridad tales como: ISO 27001, SOC 2, PCI DSS Level 1 y FISMA.

Sin embargo, hay que tener en cuenta que el ayuntamiento titular de los datos está sometido al cumplimiento del Esquema Nacional de Seguridad (ENS) de acuerdo con lo que prevé la disposición adicional primera de la LOPDDDD. En caso de que se analice, aunque ClassDojo cuenta en su web con un documento (https://www.ClassDojo.com/ca-es/security/) donde detalla diferentes aspectos de seguridad, tal y como se ha recogido en el fundamento jurídico II de este dictamen, no se ha podido verificar que el proveedor cumple con todas las medidas de seguridad que se deriven del ENS.

En cuanto a las violaciones de seguridad establece que el proveedor debe informar al centro sin demora indebida después de tener conocimiento de una violación de seguridad de los datos y se somete al procedimiento establecido en el aparato del acuerdo que regula los incumplimientos.

El punto noveno bajo el título en inglés *"Assistance"* establece que el proveedor debe proporcionar asistencia razonable en el centro escolar en el cumplimiento de las obligaciones de la normativa de protección de datos respecto a: 1) el cumplimiento de las solicitudes para ejercer los derechos de los interesados, 2) responder a consultas o quejas de los titulares de los datos 3) responder a

investigaciones y consultas de las autoridades de control, 4) notificar las violaciones de datos personales de los datos de los estudiantes del centro escolar, y 5) consultas previas con Autoridades de control Recoge el compromiso del proveedor de informar al centro escolar si cree que una instrucción viola la normativa de protección de datos. Se da cumplimiento a las obligaciones de garantizar el ejercicio de los derechos de los interesados. No obstante, se echará de menos una previsión sobre el sometimiento a las auditorías que determine el responsable o, como mínimo, el conocimiento por parte del responsable de las auditorías independientes a las que se someta la plataforma.

En este apartado se recoge también una previsión en el sentido de que, salvo que esté prohibido por la UE o las leyes de los estados miembros de la UE y sujeto a un procedimiento específico el proveedor debe informar inmediatamente al centro escolar si recibe una sola licitud de las fuerzas de la orden, los tribunales o cualquier gobierno o cualquier entidad, de acceder a datos personales y, en cualquier caso, se prevé expresamente que si se requiere un informe de la LEA. Provider must consulta y cumple con las instrucciones de la competente Supervisory Authority".

Aunque el pacto cuarto de la adenda de privacidad prevé que el proveedor tendrá que eliminar todos los datos del estudiante cuando lo solicite el centro escolar, se echa de menos la concreción respecto al destino que se dará a las datos una vez finalizado el encargo del tratamiento en este pacto séptimo.

Por tanto, se puede concluir que no se puede garantizar que el uso de esta aplicación cumple la normativa de protección de datos dadas las carencias analizadas relativas, entre otras, a disponer de una política de privacidad fácilmente accesible y entendedora, a ofrecer garantías suficientes en cuanto a las transferencias internacionales de datos, a garantizar el cumplimiento de las medidas de seguridad del ENS o que el responsable del tratamiento pueda oponerse a la subcontratación de servicios a terceras empresas.

Conclusiones

El centro educativo o, en su caso el ayuntamiento del que dependa la guardería, es el responsable del tratamiento de los datos de los alumnos y de los padres, mientras que las empresas proveedoras de las aplicaciones objeto de la consulta serían encargados del tratamiento de estos datos.

La utilización de las aplicaciones para la comunicación con los padres ligada al ejercicio de las funciones educativas y orientadoras puede encontrar cobertura en el artículo 6.1.e) en relación con las previsiones de la LOE. En caso de que el tratamiento se quiera basar en el consentimiento, para que éste sea válido, los padres deben disponer de alternativas para poder seguir la agenda y las comunicaciones de la escuela, sin que ello les comporte un perjuicio .

Los principales riesgos derivados de la utilización de estas aplicaciones están relacionados con la correcta implantación de medidas de seguridad que eviten la alteración, pérdida, tratamiento o acceso no autorizado a los datos, a la implantación de medidas que garanticen a los titulares de los datos obtener información sobre el tratamiento y el ejercicio de los derechos y el control de sus datos, en especial los derivados de la utilización del cloud computing y la transferencia internacional de datos.
A estos efectos y para identificar y en su caso mitigar los riesgos existentes, resulta altamente recomendable realizar una evaluación de impacto relativa a la protección de datos.

Respecto a la consulta sobre si la utilización de estas aplicaciones cumple la normativa de protección de datos debe tenerse en consideración que el responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto de la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo que establece el RGPD, y que garantice la protección de los derechos de las personas afectadas.

Con la información facilitada y la obtenida de Internet no se dispone de datos suficientes para determinar si la aplicación Dinantia ofrece las garantías necesarias que se requiere de un encargado del tratamiento.

En cuanto a la aplicación ClassDojo, aunque la información ofrece mayores garantías de adecuación al RGPD que la obtenida en el caso de Dinantia, existen determinadas carencias, concretadas en los fundamentos jurídicos VII y VIII de este dictamen, que impiden concluir a partir de la información disponible, la adecuación al RGPD.

Barcelona, 25 de febrero de 2021