Principios básicos para la contratación y uso de plataformas educativas digitales por las administraciones educativas y centros docentes

aepd agencia española protección datos

apdcat Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Consejo de Transparencia y Protección de Datos de Andalucía

Guía publicada en
marzo 2026

I. Introducción

La utilización de plataformas educativas digitales en la nube presenta riesgos y desafíos específicos en el contexto del marco jurídico de protección de datos personales. Así se ha puesto de manifiesto en diversos pronunciamientos de las autoridades de protección de datos, esto es, la Agencia Española de Protección de Datos, la Autoritat Catalana de Protecció de Dades, la Autoridad Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía, centrados en aspectos esenciales del Reglamento General de Protección de Datos (RGPD): los principios del tratamiento, las obligaciones de transparencia e información, los requisitos del encargo de tratamiento, la evaluación de impacto y el análisis de riesgos, la protección de datos desde el diseño y por defecto, el ejercicio de derechos y las garantías en materia de transferencias internacionales. Problemáticas similares han sido identificadas por autoridades de control de otros Estados miembros de la Unión Europea.

El presente texto establece unos principios básicos consensuados entre las autoridades de control y dirigidos a los distintos agentes y operadores que mediante plataformas tecnológicas tratan datos personales en el ámbito de la educación.

II. El entorno educativo digital y la protección del menor

Las plataformas educativas digitales permiten al alumnado, al profesorado y a las familias interactuar y colaborar en línea con fines educativos. Su implantación responde al mandato legal de desarrollar la competencia digital del alumnado y facilitar la función docente.

La contratación de estas plataformas entraña una responsabilidad singular. Los principales afectados son, en gran medida, personas menores de edad que merecen una protección específica de sus datos personales (considerando 38 RGPD). Y la dimensión del tratamiento es extraordinaria: estas plataformas pueden afectar simultáneamente a millones de menores. El interés superior del menor exige un escrutinio reforzado de cualquier tratamiento que les afecte.

A esta circunstancia se añade que la utilización de la plataforma no es voluntaria para el alumnado ni para sus familias, sino que constituye la herramienta institucional facilitada para el ejercicio de la función educativa, con una posterior adhesión a la misma por parte de los alumnos, padres, madres o tutores.

III. Naturaleza de las plataformas educativas digitales y sujetos y roles implicados

Estas plataformas están compuestas por un conjunto de aplicaciones y servicios en la nube, proporcionados por proveedores tecnológicos externos, que ofrecen funcionalidades de evaluación y registro del progreso del alumnado, comunicación, almacenamiento, edición colaborativa y otras relacionadas con la gestión del aula. Desde la perspectiva de la protección de datos, resulta imprescindible distinguir tres dimensiones.

En cuanto a los servicios, las plataformas incluyen servicios básicos directamente vinculados a la función educativa, como aulas virtuales, espacio de almacenamiento, comunicación, tutoría o videoconferencia. Junto a ellos, ofrecen servicios adicionales u optativos que pueden no guardar relación directa con dicha función educativa, como buscadores, plataformas de vídeo o herramientas de inteligencia artificial, si bien se ofrecen a los afectados de manera conjunta en el momento de la adhesión. Sin embargo, estos últimos servicios pueden regirse por condiciones contractuales diferenciadas y pueden estar fuera del ámbito del encargo de tratamiento. Asimismo, y en ocasiones, el proveedor puede actuar respecto de ellos como responsable del tratamiento para fines propios.

En cuanto a los datos, conviene diferenciar los datos que los usuarios proporcionan o generan en el uso de la plataforma (documentos, comunicaciones, calificaciones, trabajos, en su caso, pautas o hábitos de uso de la plataforma) de los datos recogidos y generados automáticamente por el uso y funcionamiento de la propia plataforma (direcciones IP, identificadores de dispositivo, datos de localización, registros de actividad, cookies, metadatos de uso e interacción). El tratamiento de estos últimos puede escapar al conocimiento detallado y al control efectivo del responsable.

En cuanto a los roles, la posición del proveedor no admite una calificación única. Puede actuar como encargado del tratamiento respecto de los datos proporcionados o generados por los usuarios en los servicios básicos, conforme a las instrucciones del responsable. Sin embargo, puede actuar simultáneamente como responsable del tratamiento en al menos dos supuestos: cuando determina por sí mismo los fines y los medios del tratamiento de los datos recogidos y generados automáticamente por el uso y funcionamiento de la propia plataforma, y cuando presta servicios adicionales totalmente ajenos a la función educativa para fines propios. La determinación del rol debe atender, en cada caso, a quién decide efectivamente sobre los fines y los medios del tratamiento, valorando las funciones que le atribuyan los términos del contrato y sin perjuicio de las previsiones del artículo 33.2 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que considera responsable a quien actúa en nombre propio o utiliza los datos para finalidades propias aun cuando figure formalmente como encargado, al margen de las singularidades derivadas de la contratación pública.

IV. Principios básicos

1 Pleno respeto a los derechos y libertades en el tratamiento de datos personales

El tratamiento de datos personales derivado del uso de plataformas educativas digitales debe respetar íntegramente los derechos y libertades fundamentales de las personas interesadas, en particular de los menores de edad. Cualquier tratamiento que les afecte debe valorarse desde el interés superior del menor como consideración primordial.

La circunstancia de que la plataforma se ofrezca de forma gratuita a las administraciones educativas no puede suponer, directa ni indirectamente, una merma en el nivel de protección de los datos personales del alumnado, de sus familias ni del profesorado.

2 Determinación clara de la responsabilidad del tratamiento

Las administraciones educativas y los centros docentes deben asumir de forma proactiva y efectiva su condición de responsables del tratamiento, sin delegar ni diluir dicha responsabilidad.

Cuando la plataforma se ponga a disposición de los centros por la administración educativa, deberá determinarse con claridad la distribución de funciones y, en su caso, responsabilidades entre ambos niveles.

3 Bases de legitimación y estricta limitación de finalidades

El tratamiento de datos personales derivado del uso de la plataforma educativa debe contar con una base de licitud válida para cada finalidad y cada responsable del tratamiento.

3. Bases de legitimación y estricta limitación de finalidades

Los tratamientos realizados por las administraciones educativas y los centros docentes en el ejercicio de la función educativa encuentran su base legitimadora en la misión en interés público (art. 6.1.e RGPD), de conformidad con la legislación educativa aplicable. Esta base ampara exclusivamente los tratamientos derivados del ejercicio de dicha función. Cualquier tratamiento que exceda de esa finalidad requiere de una justificación propia.

Los servicios adicionales u optativos ofrecidos a través de la plataforma que no respondan a la función educativa, ni sean necesarios para la educación y orientación del alumnado, no deben activarse en un entorno institucional dirigido a menores. La implantación obligatoria de la plataforma no puede convertirse en un canal para ofrecer al alumnado servicios ajenos al propósito educativo. Solo cuando un servicio adicional presente relación con la función educativa podrá valorarse su activación por la administración educativa y los centros docentes, que deberán justificar dicha vinculación e incluir el tratamiento en la evaluación de impacto correspondiente. Respecto de los datos generados automáticamente por el uso y funcionamiento de la plataforma, cuando el proveedor los trate para finalidades ajenas a la función educativa, dichos tratamientos requieren una base de licitud propia y autónoma.

En un contexto de uso de la plataforma por parte de los menores para funciones relacionadas con la finalidad educativa, el interés legítimo del proveedor (art. 6.1.f RGPD) difícilmente puede constituir una base adecuada o en general suficiente para tratamientos que persigan finalidades comerciales, de mejora de productos o servicios, publicidad, perfilado o analítica para fines propios del proveedor. El artículo 6.1.f del RGPD exige, cuando el interesado sea un niño o niña, una ponderación especialmente rigurosa que, para estas finalidades, no puede resolverse por regla general a favor del interés comercial del proveedor ajeno a la finalidad educativa frente a los derechos y libertades de los menores (considerando 38 RGPD).

Así las cosas, con carácter general resultarán admisibles aquellos tratamientos de datos por parte de la plataforma educativa, en el ámbito del encargo, generados automáticamente que sean estrictamente necesarios para la prestación técnica y segura del servicio contratado. En los casos particulares en los que el proveedor de la plataforma actuara como responsable invocando su interés legítimo, deberá acreditar el cumplimiento del artículo 6.1.f del RGPD: la legitimidad del interés perseguido, la necesidad del tratamiento para satisfacer dicho interés y la no prevalencia de los derechos y libertades fundamentales de los interesados, con la ponderación especialmente rigurosa que exige dicho artículo cuando el interesado sea un menor.

Estos tratamientos deberán, en todo caso, respetar los principios del artículo 5 del RGPD, en particular los de limitación de la finalidad, minimización de datos y limitación del plazo de conservación.

4 Evaluación de impacto y participación del delegado de protección de datos

Con carácter previo a la puesta en funcionamiento de cualquier plataforma, el responsable deberá realizar una evaluación de impacto relativa a la protección de datos (art. 35 RGPD). El tratamiento a gran escala de datos de menores mediante tecnologías en la nube reúne múltiples elementos que la hacen obligatoria.

La evaluación de impacto debe abarcar la totalidad de los tratamientos derivados del uso de la plataforma. Deberá incluir el análisis de roles a que se refiere el principio 2, la verificación de las bases de licitud conforme al principio 3, y una evaluación específica de los riesgos para los derechos y libertades de los interesados que contemple la naturaleza, el alcance, el contexto y los fines de todos los datos tratados.

El delegado de protección de datos deberá participar, desde las fases iniciales, en el estudio, selección e implantación de la plataforma, incluyendo la propia evaluación de impacto, la revisión del contrato de encargo y la configuración del servicio.

La evaluación de impacto no es un ejercicio puntual. Deberá revisarse y actualizarse cuando se produzcan cambios significativos en las condiciones del tratamiento, como la incorporación de nuevos servicios, las modificaciones en las condiciones contractuales del proveedor, o la evolución de los riesgos identificados.

5 Transparencia e información

El alumnado, sus familias y el profesorado deben recibir información completa, accesible y comprensible sobre todos los tratamientos derivados del uso de la plataforma (arts. 12, 13 y 14 RGPD). Esta obligación abarca tanto los tratamientos realizados por el responsable como aquellos que el proveedor lleve a cabo como responsable para fines propios. No resulta suficiente la mera remisión a políticas de privacidad genéricas, dispersas en múltiples documentos o redactadas de forma que no permita conocer con precisión las finalidades, las categorías de datos tratados, los plazos de conservación ni sus destinatarios. La información debe proporcionarse con un lenguaje especialmente claro y sencillo cuando se dirija a menores de edad (art. 12.1 RGPD).

Cada responsable del tratamiento debe asumir sus propias obligaciones informativas, atendiendo al modelo organizativo implantado. Asimismo, los tratamientos derivados de la plataforma deberán estar debidamente recogidos en el registro de actividades de tratamiento (art. 30 RGPD), como presupuesto necesario para el cumplimiento de las obligaciones de transparencia.

6 Contrato de encargo de tratamiento y control de subencargados

El uso de la plataforma deberá regirse por un contrato de encargo que cumpla íntegramente con el artículo 28 del RGPD. El contrato deberá constar por escrito, ser accesible y comprensible para el responsable, y regular con precisión el objeto, la duración, la naturaleza y la finalidad del tratamiento, las categorías de datos personales y de los interesados. La documentación contractual debe permitir al responsable conocer con claridad el alcance y las condiciones del encargo. La dispersión de las condiciones en múltiples documentos con reglas de prelación complejas y susceptibles de modificación no exime al proveedor de sus obligaciones ni al responsable de las suyas.

El responsable debe conservar la capacidad real de impartir instrucciones al encargado. Las cláusulas contractuales no pueden atribuir al proveedor la facultad de modificar unilateralmente elementos esenciales del tratamiento, como las finalidades, las categorías de datos tratados, las condiciones de seguridad, el régimen de transferencias internacionales o la incorporación de nuevos servicios. Los ajustes que no alteren la sustancia del tratamiento podrán canalizarse mediante procedimientos de notificación previa al responsable. Si las condiciones del servicio o del contrato cambian con frecuencia o complejidad, de manera que el responsable no puede mantener documentada de forma continua la licitud del tratamiento, dicha circunstancia puede constituir motivo suficiente para cesar en la utilización de la plataforma o exigir la correcta ejecución del contrato.

La contratación de subencargados debe ser autorizada por el responsable (art. 28.2 RGPD). Cuando se opte por una autorización general, esta deberá ir acompañada de requisitos estandarizados de protección de datos que todos los subencargados, actuales y futuros, deban cumplir. El responsable debe conocer la identidad, la ubicación y las finalidades de los tratamientos de cada subencargado, y conservar el derecho efectivo a oponerse cuando un subencargado concreto no cumpla los estándares exigidos. El encargado deberá garantizar que los subencargados asumen idénticas obligaciones de protección de datos. El responsable deberá documentar qué mecanismos de verificación aplicará, y con qué periodicidad, para comprobar el cumplimiento efectivo por parte de los subencargados. La intensidad de esta verificación será proporcional al riesgo que el tratamiento represente para los derechos y libertades de los interesados.

El encargado debe poner a disposición del responsable toda la información necesaria para ayudarle a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD sobre la seguridad de los datos personales (art. 28.3.f RGPD), y demostrar el cumplimiento de sus obligaciones y permitir la realización de auditorías e inspecciones (art. 28.3.h RGPD). Este derecho debe ser efectivo y no

puede quedar satisfecho mediante la mera remisión a certificaciones genéricas o informes estandarizados que no permitan al responsable verificar las condiciones concretas del tratamiento.

El contrato deberá contemplar las condiciones aplicables a la finalización del servicio, incluyendo la devolución íntegra de los datos al responsable y su supresión efectiva por el encargado una vez completada dicha devolución (art. 28.3.g RGPD), y las medidas adecuadas para garantizar la continuidad en la prestación de la función educativa.

7 Garantías en transferencias internacionales

Con carácter previo a la implantación de la plataforma, el responsable deberá analizar todas las transferencias internacionales de datos que se deriven de la solución tecnológica adoptada (Capítulo V RGPD). Este análisis debe abarcar la totalidad de los flujos de datos, incluyendo los derivados de la actividad de los subencargados y del tratamiento de los datos recogidos y generados automáticamente por la plataforma.

Toda transferencia a terceros países deberá estar amparada por un mecanismo válido conforme al Capítulo V del RGPD, ya sea una Decisión de Adecuación de la Comisión Europea o mediante garantías adecuadas, en particular cláusulas contractuales tipo.

Cuando, en ausencia de una Decisión de Adecuación, se aporten garantías adecuadas mediante cláusulas contractuales tipo de la Comisión Europea, o de cualquier otro de los instrumentos previstos en el artículo 46.2 del RGPD, el responsable deberá verificar, caso por caso, si el ordenamiento jurídico del país de destino garantiza un nivel de protección sustancialmente equivalente al del Espacio Económico Europeo. Cuando dicho nivel no pueda garantizarse, deberán adoptarse medidas suplementarias eficaces. Esta evaluación deberá documentarse y mantenerse actualizada.

Las excepciones previstas en el artículo 49 del RGPD no constituyen una base adecuada para amparar transferencias sistemáticas y continuadas como las derivadas del uso habitual de una plataforma educativa.

La indeterminación sobre los flujos de datos o la falta de garantías suficientes constituye motivo bastante para no autorizar el uso de la plataforma.

8 Protección de datos desde el diseño y por defecto

La plataforma debe configurarse de modo que, en su estado inicial, solo se traten los datos estrictamente necesarios para la finalidad educativa (art. 25 RGPD). Los servicios adicionales ajenos a la función educativa deberán estar desactivados por defecto y las funcionalidades de recogida automática de datos limitadas al mínimo imprescindible.

Deberá prestarse especial atención a que la plataforma no realice ni permita técnica u organizativamente el tratamiento de categorías especiales de datos (art. 9 RGPD) salvo que concurra alguna de las excepciones previstas legalmente. Asimismo, el tratamiento de contenido fotográfico y audiovisual deberá limitarse a lo adecuado, pertinente y necesario para la finalidad educativa, estableciendo protocolos que eviten usos inadecuados y garantizando la existencia de la correspondiente base jurídica.

El proveedor debe ofrecer al responsable opciones de configuración que permitan aplicar efectivamente estos principios. El responsable deberá establecer protocolos de uso y verificación periódica que aseguren el mantenimiento de esta configuración a lo largo del tiempo.

9 Seguridad de la información

El responsable y el encargado deberán aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento para los derechos y libertades del alumnado (art. 32 RGPD), teniendo en cuenta la naturaleza de los datos tratados y la especial vulnerabilidad de los interesados.

Se deberán cumplir las medidas de seguridad del Esquema Nacional de Seguridad, cuando el responsable sea una administración pública y la plataforma encargada del tratamiento preste servicios a la misma.

El contrato de encargo deberá garantizar que el proveedor notifique al responsable las brechas de seguridad que afecten a datos personales sin dilación indebida y dentro del plazo que permita al responsable cumplir con su obligación de notificación a la autoridad de control (arts. 33 y 34 RGPD).

10 Derechos de los interesados

El responsable del tratamiento debe garantizar el ejercicio efectivo de los derechos de acceso, rectificación, supresión, limitación y oposición y a no ser objeto a decisiones automatizadas, tanto frente a los tratamientos que realice como responsable como frente a los del proveedor en calidad de encargado (arts. 15 a 22 RGPD).

Cuando la base legitimadora sea la misión en interés público o, eventualmente, el interés legítimo, deberán contemplarse mecanismos efectivos para el ejercicio del derecho de oposición (art. 21 RGPD). Si se estimase la oposición, los responsables deberán adoptar las medidas necesarias para que la persona afectada no sufra discriminación ni agravio comparativo en su derecho fundamental a la educación.

aepd
agencia
española
protección
datos

apdcat
Autoritat Catalana de
Protecció de Dades

Datuak Babesteko
Euskal Agintaritza
Autoridad Vasca de
Protección de Datos

Consejo de Transparencia
y Protección de Datos
de Andalucía