ECIJA

EU KIDS Act

Protección de menores en el entorno digital

Octubre 2026

Abierta la consulta pública en España sobre el EU KIDS Act

El Ministerio para la Transformación Digital y de la Función Pública ha sometido a consulta pública la propuesta de Reglamento EU KIDS Act. Es una ocasión para que las empresas y organizaciones afectadas trasladen su posición en una fase temprana, mientras la propuesta se tramita ante el Parlamento Europeo y el Consejo.

Plazo

Del 21 de octubre al 4 de noviembre de 2026, a las 23:59.

Cómo participar

por correo electrónico a consultapublica.normasdgosdca@digital.gob.es, indicando en el asunto “Consulta pública Reglamento EU KIDS. – Aportaciones [nombre o razón social]”.

Sobre qué

Los problemas que pretende resolver la norma, la necesidad y oportunidad de aprobarla, sus objetivos y las posibles alternativas, regulatorias o no.

A continuación se resumen sus claves para facilitar la preparación de aportaciones.



Marco regulatorio

La Comisión Europea adoptó el 17 de septiembre de 2026 la propuesta de Reglamento EU KIDS Act (EU Keeping Internet Digital Spaces Accountable and Trustworthy), COM(2026) 681.

Finalidad:

garantizar un nivel elevado y uniforme de protección de los menores en línea en toda la Unión y evitar la fragmentación del mercado interior derivada de las iniciativas nacionales.

Alcance territorial:

aplica con independencia del lugar de establecimiento del proveedor, siempre que preste servicios a usuarios situados en la UE.

Complementa:

el Reglamento (UE) 2022/2065 de Servicios Digitales (DSA), en concreto su art. 28 sobre protección de menores, y el Reglamento (UE) 2024/1689 de Inteligencia Artificial (AI Act). En esta nota, "RGPD" remite al Reglamento (UE) 2016/679.

Proveedores no establecidos en la UE:

obligación de designar un representante legal, salvo tiendas de aplicaciones y sistemas operativos. No se prevé exención para pymes.

Aplica a:

proveedores de servicios de redes sociales en línea, plataformas de intercambio de vídeos, tiendas de aplicaciones, juegos en línea, sistemas operativos, acompañantes de IA (AI companions) y chatbots de propósito general accesibles a menores de 18 años.

VLOPs:

plataformas en línea de muy gran tamaño, es decir, las que alcanzan al menos 45 millones de usuarios activos mensuales en la UE y han sido designadas como tales conforme al art. 33 DSA. Quedan sujetas a obligaciones reforzadas.

Plazos de aplicación ↘

*Nota: los plazos pueden cambiar durante la tramitación. Las fechas concretas se conocerán con la publicación del texto definitivo en el DOUE.

Hay dos fechas de referencia:

1. La **entrada en vigor** se produce 20 días después de su publicación en el DOUE.
2. La **fecha de aplicación** llega 6 meses más tarde, y es a partir de ella cuando las obligaciones son exigibles con carácter general.

A. Plazos que se cuentan desde la entrada en vigor:

Día de la entrada en vigor: las VLOPs de redes sociales y plataformas de vídeo quedan obligadas a elaborar un plan de cumplimiento y someterlo a una auditoría independiente. El plazo para notificar ese plan se cuenta, sin embargo, desde la fecha de aplicación (ver bloque B).

12 meses después de la entrada en vigor: se aplican el procedimiento acelerado de la Comisión y la obligación de los Estados miembros de adoptar medidas nacionales de apoyo a los menores. Este hito no añade obligaciones a las empresas.

B. Plazos que se cuentan desde la fecha de aplicación

Fecha de aplicación (6 meses después de la entrada en vigor): todos los proveedores incluidos, salvo los sistemas operativos, deben cumplir las obligaciones de seguridad desde el diseño. Las redes sociales y plataformas de vídeo con funcionalidades de riesgo deben, además, aplicar las edades mínimas y verificar la edad al crear nuevas cuentas.

30 días después de la fecha de aplicación: las VLOPs ya designadas notifican su plan de cumplimiento a la Comisión. Las que se designen más tarde disponen de 4 meses desde su designación.

6 meses después de la fecha de aplicación: las redes sociales y plataformas de vídeo deben haber revisado las cuentas existentes (ver apartado 4).

¿Por qué es relevante?

ES: un marco armonizado en toda la UE que impone obligaciones de diseño de producto, de verificación de edad y, para las VLOPs, de acreditación proactiva del cumplimiento.

NO ES: una declaración programática ni una obligación que pueda atenderse únicamente mediante la revisión de los términos y condiciones.

SUJETOS OBLIGADOS

Redes sociales en línea

Plataformas de vídeo

Tiendas de aplicaciones

Videojuegos en línea y plataformas de videojuegos

Sistemas operativos (deben facilitar el intercambio de la señal de edad, previo consentimiento del usuario)

AI companions y chatbots de propósito general*

*Nota: quedan fuera los chatbots con funciones especializadas, entre otros los de servicio al cliente, operaciones comerciales, apoyo técnico, transaccionales, educativos, de recuperación de información, industriales o de fabricación.

EXCLUIDOS

Enciclopedias en línea sin ánimo de lucro

Repositorios educativos y científicos sin ánimo de lucro

Servicios y sistemas diseñados principalmente con fines educativos y utilizados por centros u organizaciones educativos, o en su nombre

Plataformas de código abierto, salvo que constituyan un sistema de IA en el ámbito del EU KIDS Act o del AI Act

Servicios destinados exclusivamente a investigación científica

Servicios y sistemas diseñados, desarrollados y utilizados por autoridades públicas y para su uso exclusivo o en su nombre

Zona gris: no se define “centro u organización educativa”, lo que genera incertidumbre para las plataformas de aprendizaje y los videojuegos con finalidad educativa.

Acceso por edad

Menores de 13 años:

no podrán disponer de cuenta en redes sociales. En plataformas de vídeo, solo podrán acceder a servicios diseñados específicamente para ellos, a través de la cuenta del titular de la responsabilidad parental y con control parental.

13 y 14 años:

si el proveedor lo permite, cuentas de funcionalidad limitada creadas por el titular de la responsabilidad parental, con las siguientes condiciones:

- Límite diario de uso fijado por el tutor, que no podrá exceder de una hora.
- Posibilidad de que el tutor preautorice nuevos contactos y limite su número.
- Herramientas de supervisión permanentemente activas.

15 años o más:

cuenta autónoma, sujeta a las obligaciones de seguridad desde el diseño aplicables a todos los menores de 18 años.

¿A quién afectan estas restricciones?

A las redes sociales y plataformas de vídeo que incorporen alguna de estas funcionalidades de riesgo:

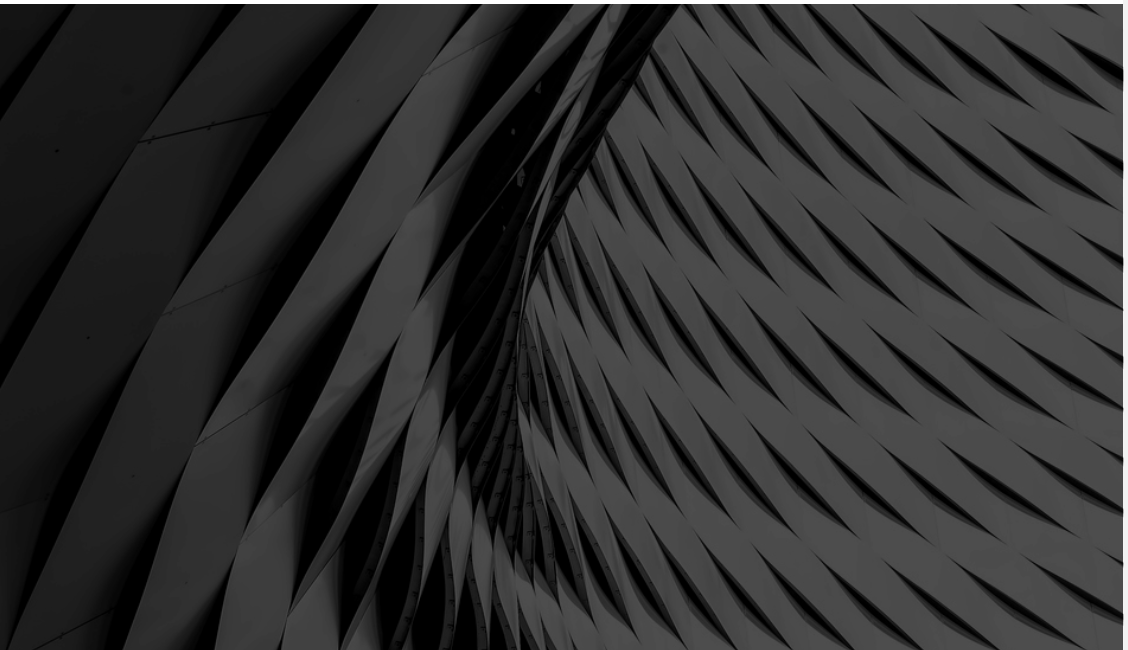
- Retransmisión en directo.
- Contacto con usuarios ajenos a las conexiones previas.
- Sistemas de recomendación basados en perfilado o sugerencias de contactos.
- Diseños orientados al consumo continuo o notificaciones de reenganche.

¿Qué ocurre con las cuentas existentes?

- **Plazo:** 6 meses desde la aplicación para determinar si los titulares son menores de 15 años.
- **Desactivación:** cuentas de menores de 15 años y aquellas cuya edad no pueda determinarse.
- **Excepción:** no será necesaria la verificación cuando pueda acreditarse con un alto grado de confianza que el titular supera esa edad (por ejemplo, por la antigüedad de la cuenta).

Seguridad desde el diseño

Protección por defecto: todos los servicios, salvo los sistemas operativos, deben diseñarse por defecto conforme a las obligaciones de protección de menores, también para los usuarios no registrados. Solo podrán establecerse excepciones cuando se haya determinado, mediante garantía de la edad, que el usuario es adulto. Además, ningún proveedor podrá eludir sus obligaciones. Por ejemplo, al crear la cuenta no podrá pedirse al menor que reduzca su nivel de privacidad, y deberá limitarse la creación de cuentas secundarias.



Obligaciones específicas de redes sociales y plataformas de vídeo:

Diseño adictivo: se prohíben:

- La reproducción automática y el consumo ininterrumpido de contenidos, como el desplazamiento infinito (infinite scroll).
- Las notificaciones de reenganche.
- Los incentivos a compartir contenidos o emitir en directo y las penalizaciones por no interactuar con regularidad.

Gestión del tiempo de uso:

medidas eficaces que limiten la duración del acceso y permitan interrumpir el uso.

Franjas protegidas:

esas medidas deben proteger el horario escolar y las horas centrales de sueño, es decir, al menos ocho horas consecutivas entre las 22:00 y las 08:00. Las notificaciones push también deben respetar esas franjas.

Sistemas de recomendación:

prioridad a las preferencias explícitas del usuario y desactivación por defecto de las recomendaciones basadas en señales implícitas de interacción. Además, prohibición de usar datos recabados fuera del servicio, posibilidad de borrar las preferencias y al menos una opción no basada en perfilado.

Configuración por defecto:

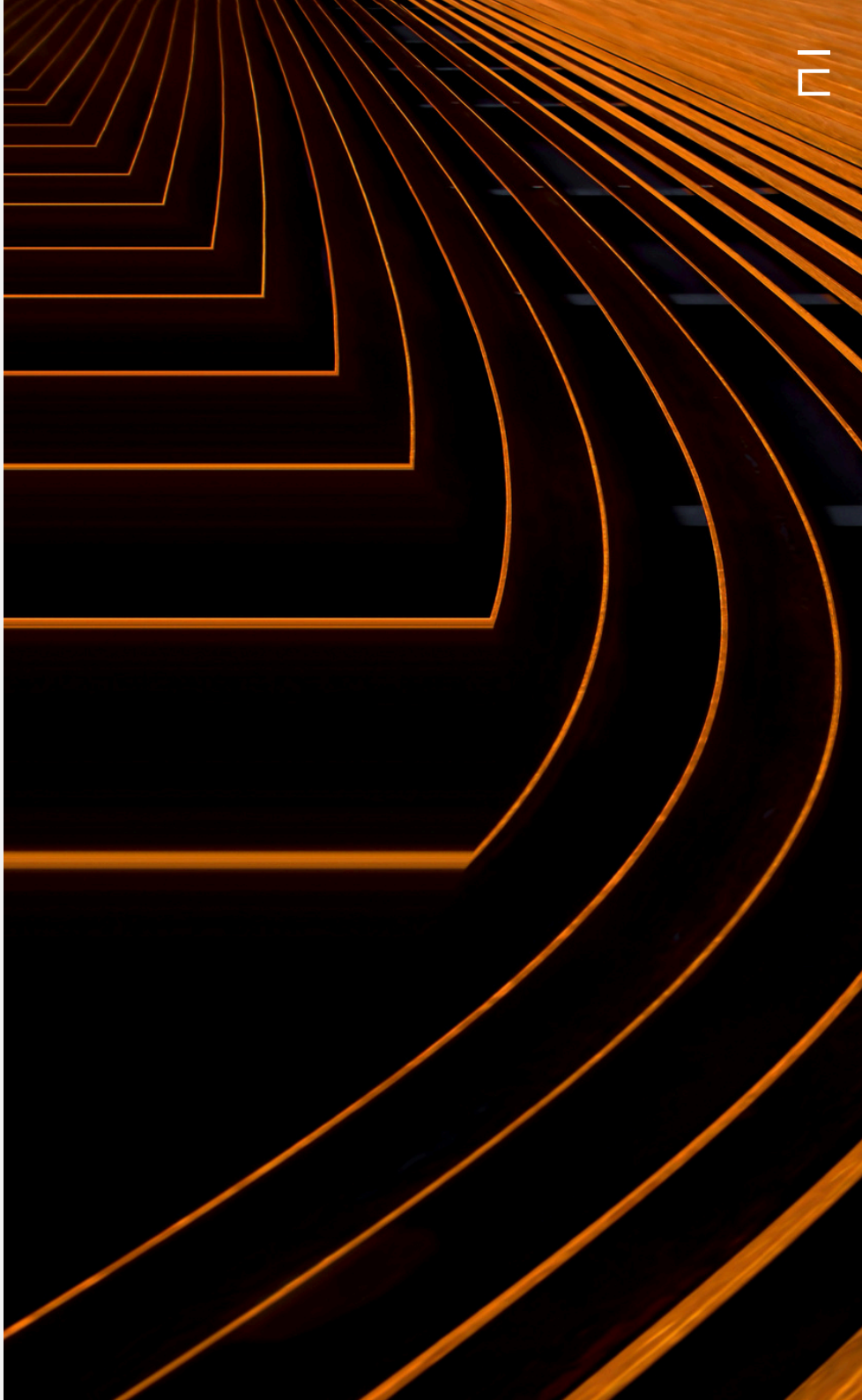
- Desactivación por defecto de la geolocalización, el micrófono, la cámara, la recomendación de otras cuentas, la sincronización de contactos y las notificaciones push.
- Exclusión de las funciones que tergiversen la imagen del menor, en especial mediante su embellecimiento o idealización desproporcionados.
- Exclusión de las funciones que aumenten la comparación social, como permitir ver el número de reacciones a sus contenidos.

Contactos y visibilidad:

- Ningún usuario podrá contactar directamente con el menor sin su aprobación previa, y el menor no aparecerá en las sugerencias de contactos.
- Perfil y contenidos del menor no visibles por defecto para usuarios no aceptados.
- Prohibición de descargar o capturar los contenidos del menor.
- Emisión en directo desactivada por defecto.

Transacciones económicas:

- Aviso claro y en tiempo real, antes de cada transacción, de que se trata de una transacción económica.
- Precio en moneda nacional cuando se utilicen monedas virtuales.
- Prohibición de diseños que puedan conducir a gastos excesivos, impulsivos o no deseados, incluida la exposición a sistemas de recompensa variable, como las cajas de recompensas o loot boxes.



IA y menores

Los acompañantes de IA y los chatbots de propósito general accesibles a menores quedan sujetos a las siguientes obligaciones:

Dependencia emocional:	se prohíben las características y comportamientos del sistema que simulen relaciones interpersonales susceptibles de crear dependencias emocionales.
Memoria de interacciones:	por defecto, no podrán utilizar información derivada de interacciones previas del menor, salvo cuando resulte necesario para proteger su seguridad.
Evaluación y seguimiento:	evaluación de riesgos con carácter previo a la comercialización y seguimiento posterior (las micro y pequeñas empresas quedan exentas de este último).
Chatbots integrados:	en redes sociales, plataformas de vídeo y videojuegos, no podrán activarse automáticamente ni mostrarse de forma destacada, no se animará a los menores a utilizarlos y estos podrán desactivarlos en cualquier momento.
Códigos de conducta:	los proveedores que se adhieran a un código considerado adecuado por la Comisión podrán basarse en él para demostrar el cumplimiento.

¿Cuándo existe riesgo de dependencia emocional?

Cuando el sistema muestra comportamientos o simula emociones o relaciones interpersonales que pueden crear dependencias, en particular si afectan a las relaciones del menor con otras personas.

Videojuegos y tiendas de aplicaciones

Videojuegos

- Prohibición de funcionalidades que fomenten el uso compulsivo o excesivo del juego, como las recompensas o penalizaciones que incentiven jugar a intervalos regulares.

- Configuración segura por defecto y salvaguardas frente a contactos de riesgo.
- Salvaguardas para evitar que el juego se utilice para incitar a los menores a iniciar contactos en otros servicios de riesgo.

- Acceso obligatorio a herramientas para tutores. El acceso de menores de 13 años solo podrá activarse y controlarse a través de ellas.

- Las plataformas que permitan a los usuarios crear juegos deberán facilitarles el cumplimiento.

- Las loot boxes y la transparencia del precio de las monedas virtuales no se imponen directamente, sino que se remiten a los códigos de conducta.

Clasificación por edades:

la Comisión fomentará la elaboración de códigos de conducta a escala de la UE, tomando como referencia los marcos paneuropeos de clasificación existentes, como PEGI. Los proveedores que se adhieran a un código considerado adecuado podrán basarse en él para demostrar el cumplimiento.

Tiendas de aplicaciones:

obligación de implantar un sistema de clasificación por edades, impedir el acceso y la compra de aplicaciones inadecuadas por menores y permitir la solución europea de verificación de edad.

Verificación de edad ↘

La autodeclaración de edad deja de considerarse un mecanismo válido de comprobación. El método exigido depende del tipo de servicio y de la obligación que se trate de cumplir:

Acceso a redes sociales y plataformas de vídeo:

verificación de edad obligatoria en el momento de creación de la cuenta, mediante una solución de verificación de la edad de la UE certificada e incluida en las listas de la Comisión. También se admiten las Carteras Europeas de Identidad Digital que cumplan esos requisitos. Ninguna otra solución, incluida la estimación de edad, resulta suficiente.

Resto de obligaciones y tiendas de aplicaciones:

se admiten otras soluciones de garantía de la edad, incluida la estimación de edad, siempre que el proveedor pueda demostrar que cumplen los requisitos de precisión, fiabilidad y privacidad que se indican a continuación. Sus requisitos se concretarán mediante actos delegados.

Privacidad:

las soluciones deberán ofrecer un alto nivel de precisión, fiabilidad, protección, solidez, no intrusión, privacidad y no discriminación. No podrán permitir identificar, localizar, rastrear ni elaborar perfiles del usuario, tratarán solo los datos estrictamente necesarios y deberán ser una prueba de conocimiento cero.

Derechos del usuario:

la señal de edad podrá conservarse en la cuenta para no repetir la comprobación, y el usuario podrá reclamar gratuitamente frente a un resultado erróneo.

Estados miembros:

deberán ofrecer gratuitamente al menos una solución de verificación de edad y un medio electrónico para acreditar la responsabilidad parental.

Responsabilidad parental:

- **Señales oficiales o propias:** bases de datos o interfaces oficiales de los Estados miembros, o señales de las que el proveedor ya disponga por interacciones previas.
- **Autodeclaración:** admitida al menos hasta que la Comisión concrete las señales válidas mediante acto delegado, acompañada de “esfuerzos razonables” de verificación por parte del proveedor, concepto aún no definido.

Supervisión y sanciones

El EU KIDS Act no crea un sistema de supervisión propio. Se apoya en el del DSA y en el del AI Act, y añade obligaciones específicas para las VLOPs.

Autoridades competentes:

la Comisión, en exclusiva, respecto de las VLOPs y de los acompañantes de IA y chatbots bajo su competencia. En los demás casos, los Coordinadores de Servicios Digitales (art. 49 DSA) y las autoridades del AI Act, así como las autoridades de protección de datos (art. 51 RGPD) en materia de verificación de edad.

Obligaciones reforzadas de las VLOPs:

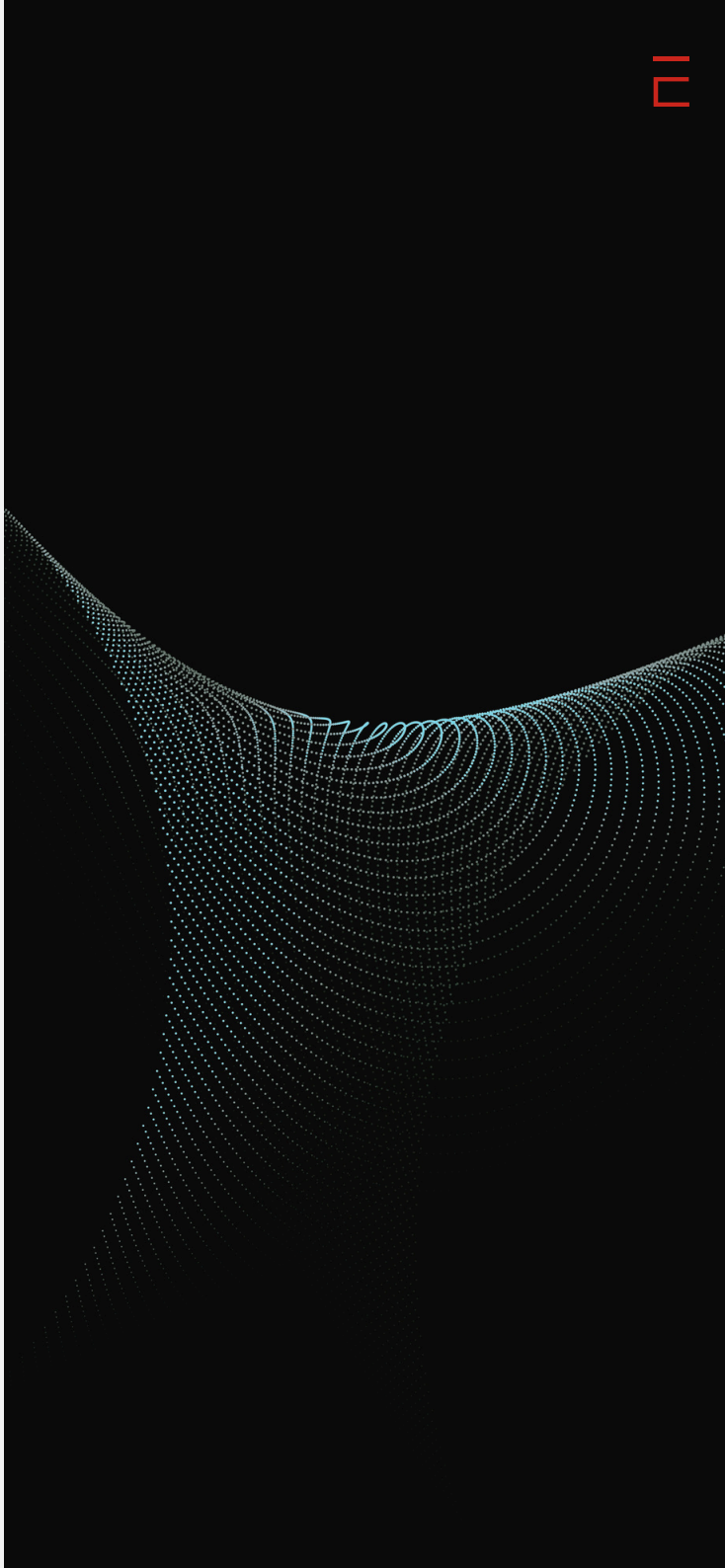
plan de cumplimiento, auditoría independiente y publicación de un resumen del informe.

Deficiencias:

plan correctivo en 30 días desde la resolución de la Comisión y aplicación de cada medida en un máximo de 60. Un informe favorable no acredita, por sí solo, el cumplimiento.

Tasa de supervisión:

la Comisión cobrará una tasa anual a las VLOPs que sean redes sociales, plataformas de vídeo o tiendas de aplicaciones, y a los acompañantes de IA, chatbots y plataformas de videojuegos que supervise. No podrá superar el 0,03% de los ingresos netos anuales mundiales del ejercicio anterior y seguirá los principios del art. 43 DSA.





Procedimiento acelerado:

la Comisión procurará adoptar una decisión final en 90 días hábiles desde la apertura del procedimiento y comunicar antes sus conclusiones preliminares.

Sanciones:

el EU KIDS Act no fija multas propias. Remite al régimen de otra norma según el tipo de servicio:

- Redes sociales, plataformas de vídeo, plataformas de videojuegos y tiendas de aplicaciones: multas de hasta el 6% del volumen de negocios anual mundial del ejercicio anterior (arts. 52.3 y 74.1 DSA). Las impone la Comisión a las VLOPs y la autoridad nacional en los demás casos.

- Acompañantes de IA y chatbots de propósito general: multas del art. 99 AI Act de hasta el 6% del volumen de negocios total anual mundial del ejercicio anterior, cuando haya dolo o negligencia.

- Protección de datos en la garantía de la edad: las autoridades de protección de datos podrán imponer multas del art. 83 RGPD de hasta 20 millones de euros o el 4% del volumen de negocios total anual mundial del ejercicio anterior, si esta cifra es mayor (art. 83.5 RGPD).

- Videojuegos que no sean plataformas: cada Estado miembro fijará las sanciones conforme al art. 52 DSA, con el mismo límite máximo del 6%. Será competente la autoridad del Estado del establecimiento principal del proveedor.

Acciones colectivas:

el EU KIDS Act se incorpora al anexo I de la Directiva (UE) 2020/1828 de acciones de representación, por lo que las entidades cualificadas podrán ejercitar acciones de representación. Además, menores y tutores podrán mandatar a entidades sin ánimo de lucro para ejercer sus derechos.

¿Quién debe hacer qué?

Obligaciones comunes (todos los servicios incluidos, salvo sistemas operativos)

- Aplicar por defecto las protecciones para menores, también a los usuarios no registrados.

- Garantizar desde el diseño un elevado nivel de privacidad, seguridad y protección de los menores.

- Comprobar mediante garantía de la edad que el usuario es adulto antes de habilitar funciones menos protectoras.

Obligaciones específicas según el tipo de servicio

• Redes sociales y plataformas de vídeo:

- Impedir que los menores de 15 años creen o utilicen cuentas propias cuando el servicio presente funcionalidades de riesgo.
- Si lo desean, habilitar cuentas limitadas creadas por el tutor para menores de 13 y 14 años.
- Verificar la edad al crear la cuenta mediante una solución certificada.
- Revisar las cuentas existentes en el plazo de 6 meses desde la aplicación.

VLOPs:

- Notificar el plan de cumplimiento a la Comisión y someterlo a auditoría independiente.
- Presentar el plan de revisión de cuentas con evidencia estadística y abonar la tasa de supervisión.

Videojuegos:

- Adoptar medidas frente al uso compulsivo o excesivo del juego.
- Establecer salvaguardas frente a contactos de riesgo.
- Garantizar el acceso a herramientas para tutores.
- Valorar la adhesión a los códigos de conducta, en los que podrán basarse para demostrar el cumplimiento.

Acompañantes de IA y chatbots:

- Evaluar los riesgos antes de la comercialización y realizar un seguimiento posterior.
- Evitar diseños que simulen relaciones interpersonales.
- No utilizar por defecto las interacciones previas del menor.

Tiendas de aplicaciones:

- Implantar un sistema de clasificación por edades.
- Impedir el acceso y la compra de aplicaciones inadecuadas por menores.
- Permitir la solución europea de verificación de edad.

Sistemas operativos:

- Facilitar el intercambio de la señal de edad con otros proveedores, previo consentimiento del usuario.

Consecuencias prácticas:

Proveedores que se anticipen

seguridad jurídica, previsibilidad y menor riesgo de rediseños urgentes.

Proveedores que esperen a la aplicación

mayor exposición a requerimientos de información, investigaciones y sanciones, y menor margen para adaptar sus servicios.

Marcas y anunciantes:

sin obligaciones directas, pero con menor alcance de las campañas dirigidas a menores de 15 años en redes sociales.

Próximo paso:

las empresas que quieran influir en el texto final pueden presentar aportaciones en la consulta pública hasta el 4 de noviembre de 2026.



ECIJA

The law firm of the future, today.

www.ecija.com