

The KIDS Act explained

The KIDS Act is a proposal for a Regulation on the protection of minors online.

The proposal at a glance

What does the KIDS Act do?

Two things. First, it sets common age rules for the whole EU. **It prohibits social media accounts under 13** and provides for parent-supervised accounts at 13 and 14, as well as for independent accounts from 15.

Second, **it imposes safety by design** on the services children use most, from social media and video platforms to games, AI chatbots and app stores: no addictive tricks leading to excessive use and exposure, no contact from strangers, safe settings by default and no spending traps.

Is this just a ban on social media for children?

No. The age rules are the most visible part, but most of the law is about how services are built and more importantly that they are safe in their design.

Age limits alone would leave the real underlying problem untouched: services designed to maximise children's time and attention.

The two halves work together: children gain access to the online world gradually as they grow up, and the services they access must be safe for them.

Why are you proposing an EU law, rather than leaving this to each Member State?

Because the internet does not stop at borders. Countries are adopting their own age limits and rules, which would mean a patchwork of laws: a child protected in one country and not in the next. One EU regulation gives every child the same high level of protection enforced directly at European level for the largest platforms.

The age rules

What exactly are the new age rules, and which services do they cover?

A staircase that follows how children grow up.

Under 13: no account.

From 13 to under 15: a guardian can set up a limited account and they will stay in control, with parental tools always on, a daily time limit of at most one hour, and parental approval of contacts.

From 15: young people can open their own account on services that must by law be safe for them.

The age rules apply to social networking and video-sharing services with proven risky features

Are children under 13 completely cut off from the online world?

No, but they will have no social media accounts.

One narrow possibility remains, completely in parents' hands: on video platforms designed specifically for young children, a parent may allow limited access through the parent's own account. The child has no account, personalised feeds and search are off, the parent sets a daily limit of up to one hour and can stop access at any time.

This arrangement ends at 13 when children reach the next access step.

My teenager already has an account. What happens to it?

Within six months of the rules applying, platforms must check whether existing account holders are under 15 and disable the accounts of those who are, or whose age cannot be established.

Where a platform can already tell with high confidence that a user is an adult, no new check is needed, so most adults will notice nothing.

Can't children simply lie about their age?

That is exactly what this law ends.

Today a date-of-birth box is the only barrier. Under the KIDS Act, self-declared age is explicitly not enough: Access must be gated by certified age verification, existing accounts must be checked, and underage accounts must be easy to report.

The era of signing up with a false birthday will be over.

Age verification and privacy

Will I have to show my ID card to a platform? Is this the end of online anonymity?

No, and no.

Platforms do not check identity documents and do not learn who you are. Age is verified through certified solutions independent of the platforms, including a free EU age verification app and, in time, the European Digital Identity Wallet.

These tools tell the platform one thing only: is the user above or below the age, yes or no. **The law requires 'zero knowledge proof' technology that cannot identify, locate,**

track or profile anyone.

Every Member State must offer at least one free way to prove your age, including for people without digital ID.

Will adults need to verify their age when using these services?

When providers already have an estimation of the user's age based on multiple signals such as account creation date or credit card details, there will be no age verification required for most existing users.

Safety by design: how the services themselves must change

What does the law do against addictive design?

It prohibits designing services to encourage compulsive or excessive use by minors, and names the techniques so there is no ambiguity. For minors, services may not use:

- endless autoplay and infinite scrolling without real breaks
- notifications designed to pull the child back, unrelated to anything the child did
- rewards for posting or streaming to mass audiences
- 'streak' mechanics that penalise a child for not returning every day

Services must also provide effective time limits and usage breaks, designed to protect children's sleep and school time.

How will children's feeds change?

Fundamentally. For minors, recommender systems must be optimised for safety, quality and mental health, not engagement.

- What a child actively chose to follow comes first
- personalisation based on tracking is off by default
- no data from outside the service may be used
- no "rabbit holes"

Children also get an easy feed reset and always at least one option without any profiling.

How are children protected from being approached by strangers?

Nobody can message a child without pre-approval, and services must guard against children being manipulated into giving it.

Children do not appear in contact suggestions, cannot be added to groups without agreement, and can block anyone anonymously. Their content is visible only to accepted contacts, their contact details are never disclosed, others cannot download or screenshot their content, and minors cannot livestream by default.

Are AI chatbots and 'AI companions' covered?

Yes. AI companions and chatbots accessible to minors may not use designs that simulate

human relationships in ways likely to create emotional dependency.

By default, they may not carry a child's earlier conversations into later ones. They must be tested for risks to children before launch and monitored for harm afterwards. Under-13s can use them only through parental control tools. Built into a platform or game, a chatbot may not switch on automatically, may not be pushed at children, and must be easy to turn off.

What changes in online games and app stores?

Games must also be safe by design. App stores must age-rate every app, including videogames, with a published methodology, they must not let children access or buy apps inappropriate for their age, and must carry the EU age verification app.

Parents, enforcement and timing

What does the law give parents?

Effective tools on every service in scope: setting screen time, seeing and approving contacts, managing settings, and reporting harmful content on the child's behalf.

On accounts for 13 and 14 year-olds these tools are always on.

Every Member State must give parents a free, privacy-preserving way to prove parental responsibility. The law never shifts the burden onto parents: parental tools complement providers' obligations, they do not replace them.

The Special Panel's co-chairs recommend reversing the burden of proof, so that services must prove they are safe before they can access children. Does the proposal do that?

It does exactly that.

The largest platforms – those with 45 million or more active monthly users in the EU – cannot simply declare themselves safe: Before coming into contact with children under the new rules, they must put on the table a detailed plan showing how they intend to meet every obligation of the law, and have it checked by independent auditors.

This audit needs to be paid by platforms, not taxpayers. The Commission can object to the auditor in case its independence is not ensured.

The burden of compliance proof sits with the platforms; it is not for authorities, parents or children to prove harm.

Who enforces all this, and what happens to providers that do not comply?

Enforcement for online platforms builds on the existing enforcement structures under the Digital Services Act and, for AI companions and chatbots, the AI Act.

This means that the Commission directly supervises the online platforms and AI chatbots most widely used in the EU. Digital service coordinators and national market surveillance authorities remain responsible respectively for the other services and AI systems covered by the Act.

For VLOPs, the compliance logic is reversed and the burden is on providers to show they comply: Before their services come into contact with children under the new regime, VLOPs must submit a compliance plan and show, verified by independent auditors at their own expense, they intend to meet every obligation.

AI companions and chatbots cannot be placed on the market until providers can demonstrate compliance with the new obligations under the Act and have a monitoring mechanism for emerging risks and incidents.

Fines can reach 6% of total worldwide annual turnover. An expedited procedure applies for services and systems supervised by the Commission: Preliminary findings within 30 days and a final decision targeted within 90 days, because there is no time to spare.

National authorities designated by Member States will supervise the new rules for video games that are not online platforms.

Source URL: <https://digital-strategy.ec.europa.eu/faqs/kids-act-explained>

© European Union, 2026 - [Shaping Europe's digital future](https://digital-strategy.ec.europa.eu/en)
(<https://digital-strategy.ec.europa.eu/en>) - PDF generated on 17/09/2026

Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license).
For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Source URL: <https://digital-strategy.ec.europa.eu/faqs/kids-act-explained>