

# Data Protection Commission

Children's data and  
parental consent



## What is the age of digital consent?

---

The age of digital consent is one of the best-known innovations under the General Data Protection Regulation (GDPR). It applies where an organisation offering online services processes the personal data of a child, and relies on consent as the legal basis for doing so. In those cases, processing the personal data of a child below that age will be lawful only if the consent is given by the child's parent or guardian.

In Ireland, the age of digital consent has been set at 16, meaning that for every child under that age, online service providers (e.g. a social media platform) that rely on consent as the legal basis for processing must obtain the consent of the child's parents in order to offer online services to them.

## Why do some social media apps and platforms have signup ages that are lower than 16?

---

There is a misconception that the age of digital consent means that internet and social media companies cannot collect the personal data of children under this age without parental consent, but that is not true. The GDPR requires every organisation that processes personal data to have a legal basis for doing so. However, consent is just one of six legal bases allowed by the GDPR. Other legal bases include where processing is necessary to perform a contract, to perform official functions or for the legitimate interests of the organisation doing the processing. Visit our website for more information on [legal bases for processing under the GDPR](#).

If a social media platform is using consent as their legal basis, then they will need to get parental consent for children under 16. But if they are using a different legal basis, the age of digital consent does not apply. If your child's favourite social media app or game has a sign-up age of less than 16, then the company must be using a legal basis other than consent.

All of this illustrates the importance of **carefully reviewing the social media platforms, games and other online services your child is interested in, and discussing these with your child before they sign up**. Don't just assume that a social media company needs your consent in order to collect your child's data. Equally importantly, don't assume that your child can't give away significant amounts of their own data without your consent.

## Where can I find more information about the consent requirements for different social media apps and games?

---

Organisations such as social media providers that process users' personal data are obliged to set out the information you need to know in their privacy policies and terms of service. We appreciate that these documents are often very long and can be difficult to read. Fortunately, there are online resources that provide bite-size reviews of these apps and games for parents. In Ireland, organisations such as [Webwise](#) and the [ISPC](#) provide information portals for parents which include primers on various apps and games that are popular with children. Many social media platforms themselves will have dedicated resources for parents. It's a good idea to review as many different sources as possible so that you can get the full picture. So if you find yourselves

overwhelmed by long and dense privacy notices, remember that there are resources out there that can help you make informed decisions about the apps, games and other online services that your child is using.

## When is my consent needed for my child's data to be collected online?

There is no simple answer to this question. The short answer is that your consent will be needed in Ireland if your child is below the age of 16 and the company is seeking to collect the child's data on the basis of consent. This also means that if the company is using a different legal basis, your consent won't be required even if your child is under 16.

The main thing to bear in mind is that **your consent isn't always needed for your child to create their own social media account**. You also shouldn't assume, even when you or your child clicks 'I agree' or 'I accept' to a website's terms and conditions, that consent provides the legal basis for processing under the GDPR. The company might still be relying on a different legal basis even though you are being asked to give your permission. **This is why it is very important to not simply click 'I accept' to the terms and conditions without reading them so that your child can start using the service.** You may be making a very significant decision about what that company can do with your child's data every time you click 'Agree.' Make sure you are in the know before you agree to use the service.

## Even when my consent is needed, companies seem to do only a rudimentary check. Why is this?

Under data protection law, where parental consent is needed, a company needs to make only "reasonable efforts" to check that consent has actually been given by the parent. This means that they don't have to confirm with absolute certainty that the parent has given consent. The law says that they have to check only to the extent that is "reasonable" in the circumstances.

Part of the reason for this is that there aren't yet many ways of checking parental consent which are accurate, proportionate and that actually work in practice. For example, most people would agree it would be disproportionate to require parents to provide concrete proof of guardianship (e.g. copies of birth certificates, court orders, other legal documents, etc.) just so that their child could use social media. On the other hand, simply asking the child for one parent's email address or phone number is going to be very easy for a child to get past. There's also the challenge of 'consent fatigue'. Parents who are bombarded with consent requests every time their child goes online can quickly get fed up and just say 'Yes' to everything, which puts children in more danger, not less.

This means that there are a lot of different issues to be balanced when organisations decide how to check parental consent online. It's up to the social media platforms and other online services used by children to carefully consider the potential risks to children from using their service. They must have appropriate measures to get parental consent where needed. They must allow parents to stay informed about their child's online activity. If you are concerned that your child was able to create a social media or gaming account that needed your consent but did so without your

knowledge, you should raise that concern with the company itself in the first instance. If you are not satisfied with their response, for example because it feels like a standard reply and does not provide a fulsome explanation, you can make a complaint to the Data Protection Commission (DPC).

## Is it really a big deal if I lie about my child's age so that they can sign up for a social media app or game that they really want?

**Yes, it is a big deal.**

It's essential to understand that **signup ages for social media and games are not like age ratings for films and TV shows**. Age ratings will vary from country to country in line with local laws and cultural sensitivities about what content is appropriate for children. Age ratings are often advisory and give discretion to parents to decide what shows and films their children may watch.

Signup ages for online services, on the other hand, are **never** advisory. If a social media platform has a signup age of 16, this means that there are identified risks to using that service for children under that age. For their own safety, children shouldn't be allowed to use it. If you help your child sneak onto these services, you may be exposing them to danger.

Bear in mind that your child will probably watch films and TV shows only once or a handful of times. On the other hand, the risks from using an age-restricted online service are open-ended. Your child could continue to use that service every day for months or years, during which they will continue to be exposed to those risks.

For all these reasons, **you should never allow or help your child to make inappropriate use of an age-restricted online service**. It doesn't matter how benign the service may seem or how close your child is to the permitted age. At the end of the day, these rules exist to keep your child safe.

## Can my child's data be shared without my consent?

There may be situations where an organisation that has your child's data, such as a school, can share it with a third party without your or your child's express consent. Often this will be for technical reasons where they need to outsource an essential function that they can't do themselves, such as using a cloud service provider.

An example might be the educational technology that your child's school uses, such as tablets, laptops and digital learning platforms and apps, which can help your child to attend classes and submit assignments online. These kinds of tool are now a normal part of primary and secondary education. However, because your child's school doesn't make any of these devices or software themselves, they need to get them from technology companies and other organisations that provide these sorts of services.

The school doesn't need your express consent to do this because it is allowed to enter into agreements with third parties to procure services that are essential for the school to function.

Other examples might be a catering company that provides school lunches, or the security company that installs fire and smoke alarms and CCTV on school property. Schools would be unable to function if they needed the consent of every parent to do these things, even if they might involve the collection of data.

However, this also means that the school is responsible for ensuring that all of this collection and processing of your child's data is fully compliant with data protection law. It must use only responsible service providers that will treat your child's data appropriately and not use it for unauthorised purposes. It needs to be fully transparent about what they are doing with your child's data and why. If you have any concerns, you should raise them with the school in the first instance. Again, you can contact the DPC if you aren't satisfied with the school's response.

### KEY TAKEAWAYS FOR PARENTS

---

- Even though the age of digital consent in Ireland is 16, children under this age may still be able to sign up for social media without parental consent. Don't assume that your consent will always be needed if your child is under 16;
- Don't just click 'I accept' when setting up a social media or gaming account for your child. Read the terms and conditions as best you can, do some research online, and talk to your child before making a decision;
- Never lie about your child's age so that they can use an age-restricted online service. Those restrictions exist to keep your child safe;
- Your consent isn't always needed for an organisation to share your child's data with a third party. However, that organisation will need a solid legal basis for doing so, will be responsible for making sure that the third party respects data protection law, and should be fully transparent about why it is sharing this data and inform you of your rights in relation to same. You can always raise a concern with the DPC if you are still not satisfied.

