

Client alert

## Data protection

4 June 2025

### European Commission Publishes Draft Guidelines on Protection of Minors Online under Digital Services Act

Regulating access and use of online services by minors, including those provided by platforms, has recently become a top priority for regulators in the EU, UK and worldwide. On 13 May 2025, the European Commission (the **Commission**) released its draft guidelines on measures to protect minors online under the Digital Services Act (**DSA**). The goal of the guidelines is to support platforms in protecting minors from illegal content and guaranteeing their safety and privacy, as required by the DSA. The guidelines, which are addressed to all online platforms that are accessible to minors, set out the procedures for assessing risk to minors and outline the measures that providers of online platform services should put in place to address these risks and comply with Article 28 of the DSA.

#### WHICH PLATFORMS ARE ACCESSIBLE TO MINORS?

The guidelines explain that platforms must assess whether they are “*accessible to minors*” in line with the criteria set out in Recital 71 of the DSA. Under this recital, a platform is accessible to minors when (i) the online platform’s **terms and conditions** permit children to use the service; (ii) when its service is **directed at or predominantly used by minors**; (iii) or where the provider is otherwise **aware that some of the recipients of its service are minors**.

Providers of platforms that are accessible to minors must ensure a high level of “*privacy, safety and security*” for minors. They must assess the risk for minors, which may derive from interaction of minors with the platform or with other users of the platform. Platform providers should take measures to mitigate such risk.

#### MEASURES TO PROTECT PRIVACY, SAFETY AND SECURITY FOR MINORS

Risk mitigation measures may include age assurance measures, including:

- **self-declaration** which relies on the individual to provide their age or age range;
- **age estimation** techniques which allow a provider to establish that a user is likely to be of a certain age, to fall within a certain age range, or to be over or under a certain age; and
- **age verification** which relies on physical identifiers or verified sources of identification that provide a high degree of certainty in determining the age of a user.

Age verification measures will be required, for example, where minors could be exposed to the purchase of products for which national law demands a minimum age (such as alcohol, pornographic content or gambling services, but also in case a Member State would, for example, set a minimum age to access certain social media platforms). In addition, any platform posing a “*high risk*” to minors should also put in place age verification “*if these risks cannot be mitigated by other measures*”. The guidelines recommend verification through trusted government-issued IDs as an effective age verification method and also refer to the ongoing work on the so-called “EU Digital Wallet”, which should provide digital identification for everyone in the Union, as well as an EU age-verification app that is currently being developed and will allow users to prove that they are over 18 years old. The guidelines clarify that providers of online platforms accessible to minors could still use other age verification methods to comply with their obligations if they “*ensure an equivalent level of verification as the EU age verification application*”.

If strict age verification measures are not required, the guidelines recommend any services that require a user to be above a required minimum age (as it is the case with social media) to use age estimation methods, whereby a platform would check whether users are of a certain age or within a certain age range, for example through an automated analysis of behavioural and environmental data, comparing the way a user interacts on a device with other users of the same age, and metrics derived from motion analysis or by testing the user’s capacity or knowledge.

Before deciding whether to put in place any age assurance method, providers should always conduct an assessment to determine whether the chosen method is appropriate to ensure a high level of privacy, safety and security for minors on their service. The assessment should also determine whether the measure is proportionate, or the objective could be attained by other less far-reaching measures (as set out in other sections of the guidelines).

The guidelines set out examples of other compliance measures to consider, including through (i) service design; (ii) reporting, user support and tools for guardians; and (iii) governance. In addition, the guidelines refer to standards (to be developed) that may provide more granularity for compliance programmes. The measures to be implemented are illustrated through “good” and “poor” practice examples throughout the guidelines.

## CONTEXT

Both Article 28 DSA and the Commission’s draft guidelines mirror some regulatory efforts that the United Kingdom (**UK**) has undertaken to protect minors online. For example, robust age checks are a cornerstone of the [Online Safety Act 2023](#), a British counterpart to the EU’s DSA. The Office of Communications (**Ofcom**) issued several guidelines to that end, e.g., a [statement on age assurance and children’s access](#) (January 2025) and [guidance on highly effective age assurance](#) (April 2025), focusing on the so-called highly effective age assurance methods, e.g., open banking or facial age estimation. Organisations that operate in the EU and the UK may wish to align their compliance strategies for both the EU and UK framework.

At the same time, the Commission is working on a [Digital Fairness Act](#), yet another legal instrument aimed at protecting consumers, including minors, within the EU in the digital environment. A legislative proposal is expected by mid-2026.

## PUBLIC CONSULTATION

The draft guidelines, which can be found [here](#), are open for final public feedback until 10 June 2025. The Commission is seeking contributions from all stakeholders, including children, parents and guardians, national authorities, online platform providers, and experts. The publication of the final guidelines is expected by summer 2025.

Thibaut D’hulst  
Gert-Jan Fraeyman  
Andreas Reindl  
Darek Kloza

## Lawyers to contact



**Thibaut D'Hulst**  
Counsel  
tdhulst@vbb.com



**Gert-Jan Fraeyman**  
Senior Associate  
gfraeyman@vbb.com



**Darek Kloza**  
Data protection expert  
dkloza@vbb.com

Brussels  
Glaverbel Building  
Chaussée de La Hulpe 166  
B-1170 Brussels  
Belgium

Phone: +32 (0)2 647 73 50

Geneva  
2 Chemin des Mines  
CH-1205 Geneva  
Switzerland

London  
Holborn Gate  
330 High Holborn  
London  
WC1V 7QH  
United Kingdom

Phone: +44 (0)20 7406 1471

# **VAN BAEL & BELLIS**

[www.vbb.com](http://www.vbb.com)

