EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

Protecting minors online - age verification guidelines

Strategic Compliance for Communications Agencies

July 2025

THE EACA MEMBERS

GUIDELINES ON THE PROTECTION OF MINORS UNDER THE (EU) 2022/2065 DIGITAL SERVICES ACT – AGE VERIFICATION

This guide provides a focused overview of the European Commission's Guidelines on the Protection of Minors under the Digital Services Act (DSA), with an emphasis on age assurance measures. It explains when and how platforms should apply age verification or age estimation, outlines which technologies meet the Commission's criteria, and clarifies why self-declaration alone is insufficient. The briefing summarises the age verification provisions most relevant to EACA members and offers practical insights to support compliance and best practice across platforms and campaigns.

1 Introduction

In **July 2025**, the **European Commission** published its **Guidelines on the Protection of Minors under the DSA**, outlining **practical, non-binding** measures to help platforms meet the obligations of **Article 28(1).**

Age assurance is highlighted as a **key safeguard**, with **clear criteria** for when and how to **apply age verification** or **age estimation,** which **technologies** are **acceptable**, and why **self-declaration** alone is **insufficient**.

The approach is **risk-based**, requiring **stricter checks** for **high-risk content or features**, and points to **upcoming EU-standard verification tools.**

This guideline highlights the **age verification provisions most relevant to EACA members.**

2 Purpose and Importance of Age Assurance

Age assurance is a key tool for protecting minors' data privacy, safety, and mental well-being in the digital environment.

It helps to:

- **Restrict access** to age-inappropriate content (e.g., gambling, pornography),
- **Prevent adults** (including those with malicious intent) **from entering child-targeted spaces**,
- **Ensure age-appropriate design** of content, functions, and user interactions.

Three Types of Age Assurance

Method	Description	Reliability
Self-declaration	User provides their age themselves (e.g., entering date of birth)	Very low
Age estimation	Technology estimates the likely age range (e.g., facial recognition, language use, behaviour)	Medium
Age verification	Official document or trusted data source confirms age (e.g., national ID, digital ID)	High

4 When Age Verification Is Required

The Commission considers it proportionate and necessary when a platform:

🎰 Hosts **high-risk content** (gambling, pornography, alcohol)

📜 **States** an **18+ age limit** in its terms of service

💬 Offers **features** with **contact or behavioural risks** (e.g., anonymous messaging) that cannot be mitigated in less intrusive ways

⚖️ Is **legally required** to apply an age restriction

5

Approved Technologies and Good Practices

Anonymous age tokens

Generated from official ID but reveal only whether the age threshold is met.

Zero-knowledge proof & cryptographic solutions

Privacy - preserving, data - minimising verification.

Double-blind systems

The verifier does not know which platform is being accessed, and the platform does not see the user's identity.

5.1

Approved Technologies and Good Practices

EU-developed solutions

EU Age Verification Solution – under development as a bridge until the **EU Digital Identity Wallet** is available (from late 2026).

Confirms only age eligibility, shares **no other personal data.**

Interoperable, privacy-focused, intended as a **reference standard** for service providers.

When Age Estimation May Be Acceptable

📅 Where terms set 13+ or 16+ age limits

🛡️ When self-declaration is insufficient but full verification would be disproportionate

🔍 If performed by an audited third party, in a privacy-preserving and effective manner

Criteria for a Suitable Age Assurance Method

Self-declaration does not meet accuracy or robustness standards and is not acceptable alone for compliance with Article 28 DSA.

A method is proportionate and appropriate only if it meets:

Criterion	Requirements
Accuracy	Reliably determines age/age range; metrics (e.g., false positives/negatives) must be published
Reliability	Works consistently in real-world conditions
Robustness	Not easily circumvented; protects integrity of age data
Non-intrusiveness	Processes only the minimum data necessary; cannot be used for profiling or tracking
Non-discrimination	Must not disadvantage any user group (e.g., disabled users, minorities)

Obligations for Service Providers

The provider **remains responsible** for the effectiveness of the method, even if a **third-party system** is used.

They must ensure that children:

- Understand the purpose of age checks,
- Can **appeal and correct errors** in age determination,
- Receive **clear, child-friendly explanations.**

Summary

Under the guidelines, **age verification** is a core element of protecting minors online. The chosen method must match the **risk level** and features of the platform, applying the principles of **proportionality, data minimisation, child rights protection, and technical reliability.**

EU-developed solutions aim to provide a **secure, interoperable, privacy-respecting framework** for age verification in the future.

Any questions?
Please don't hesitate to contact

Dr. Mónika Magyar
EACA Senior Public Affairs and Legal Advisor
monika.magyar@eaca.eu

Laura Anna dr. Magyar
EACA Public Affairs Assistant
laura.anna.magyar@eaca.eu

EACA GUIDE