Universiteit van Amsterdam

Instituut voor Informatierecht
Institute for Information Law

DSA Observatory

A Minimum Age for Social Media: A Legal Exploration

dr. Paddy Leerssen & prof. dr. Joris van Hoboken

June 2026

A Minimum Age for Social Media: A Legal Exploration

dr. Paddy Leerssen & prof. dr. Joris van Hoboken

University of Amsterdam, Faculty of Law

Institute for Information Law (IViR)

June 2026
Amsterdam

Institute for Information Law (IViR, University of Amsterdam), 2026

The authors wish to thank the experts from relevant stakeholder organisations who generously shared their knowledge and expertise in support of this project, and the academic experts Suzanne Vergnolle, Daniel Angus, Claes de Vreese, Wouter van den Bos, Christina Eckes and Seda Gürses.

The views expressed in this report are those of the authors and do not necessarily reflect those of the organisations or individuals consulted. Responsibility for any remaining errors or omissions rests solely with the authors.

This research was funded by a grant from the Netherlands Ministry of the Interior and Kingdom Relations (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties). The views expressed in this report are those of the authors and do not necessarily reflect the official position of the Ministry.

This report was originally prepared and published in Dutch. The following text is an English translation of the original document.

Summary

The coalition agreement of the Jetten I Government states the intention to establish "[a]n enforceable European minimum age of 15 for social media, with privacy-friendly age verification for young people, as long as social media are not sufficiently safe".[1] Several legislative and policy choices remain open regarding the legal implementation of this intention. In this context, this report offers an exploration of the existing child protection rules for social media in the Netherlands, including applicable fundamental rights, as well as recent policy developments in other countries (Australia and France). This summary first discusses legislative scenarios and then policy considerations.

0.1 Legislative scenarios

A minimum age for social media can be achieved through various legal means:

Enforcement of existing frameworks: On paper, EU law already offers strong safeguards for the safety of children on social media. Of particular relevance here is the recently introduced Digital Services Act ('DSA'), which creates general obligations for platforms to ensure a high level of privacy, safety and protection of minors within their services. Under the current interpretation of child protection under the DSA, there does not appear to be a categorical minimum age for social media. Rather, there is a risk-based minimum age for unsafe services based on the specific risks involved. Furthermore, the DSA obliges platforms to effectively enforce their own contractual minimum age of 13.[2] For users aged between 13 and 16, parental consent is then required under the General Data Protection Regulation (GDPR).

Viewed in this light, the current framework already meets (a certain interpretation of) the ambitions set out in the coalition agreement, and priority can be given to enforcement. This approach can provide for a proportionate and risk-based minimum age. However, the current framework offers little support for a categorical approach, with a minimum age for all social media. Furthermore, legal certainty is limited, as many relevant standards are not explicitly provided for by law; enforcement may therefore be delayed due to a lack of evidence and/or judicial review. An additional constraint for the Dutch government is that it has little direct influence over enforcement: the European Commission acts as primary enforcer vis-à-vis large platforms, and the supplementary powers at national level lie with independent supervisory authorities (in the Netherlands: the Authority for Consumers and Markets, or ACM).

Legislative change at national level: The Netherlands could also choose to set its own statutory minimum age for social media. Similar proposals have already been put forward in other Member States, including France. However, due to the harmonisation of platform regulation at EU level, the options are limited. What is possible is a national ban on use aimed at minors. The Dutch legislature does not, however, have the power to impose obligations directly on platforms, such as age verification or other protective measures. Supervision of platforms would in principle remain harmonised via the DSA. As the supervisory authority, the European Commission has already indicated that it considers platforms responsible for compliance with such national age restrictions, in principle through the use of age verification. In this scenario, enforcement therefore remains largely dependent on the European Commission and other international partners

1 https://www.kabinetsformatie2025.nl/site/binaries/site-content/collections/documents/2026/01/30/aan-de-slag---coalitieakkoord-2026-2030/coalitieakkoord-d66-vvd-cda.pdf
2 Ibid.

Legislative change at EU level: Although the current frameworks already offer a high level of protection, legislative change at EU level could also help by clarifying and tightening up the existing framework. Possible measures include easing the burden of proof for the European Commission when enforcing minimum ages and/or streamlining age assurance obligations for (unsafe) social media platforms. Enforcement via the DSA is a natural fit (unlike, for example, the GDPR or the AVMSD), as this regulation has the most comprehensive, internationally harmonised and active supervisory framework in the field of social media and child protection. This amendment could, for example, form part of the proposal for a Digital Fairness Act (DFA), which is currently being prepared.

0.1.1 Constitutional framework: is a minimum age compatible with fundamental rights?

Given the implications for fundamental rights, caution is required when designing the minimum age

Scientific consensus is limited: While there is growing evidence of the negative effects of social media on young people, scientists remain divided on the scale and distribution of these negative effects; the balance against potential positive effects; and the effectiveness of a minimum age as a restriction. Under such conditions of (scientific) uncertainty, the government may, in principle, also act on the basis of the precautionary principle to protect children.

Risks associated with restricting the fundamental rights of the child: Minors have the right to privacy and the freedom to receive or impart information or ideas through media of their choice. This right may be restricted by law, but only for limited purposes and in a proportionate manner.

Risks to the fundamental rights of adults: The enforcement of a minimum age requires age assurance measures, which in principle restrict the privacy and freedom of information of all users, not just that of children.

We conclude that a statutory minimum age for social media may be compatible with fundamental rights, provided that care is taken to ensure proportionate implementation and enforcement. In particular, the design of age assurance measures requires caution, as this restricts the freedoms of all users, including adults.

0.1.2 Feasibility: How can age be determined?

Enforcing a minimum age on social media is challenging, since most service providers cannot reliable determine user age. To enforce a minimum age or other age-related policies, additional data must therefore be made available to platforms, which may result in privacy risks. The most important methods are:

Self-declaration by the user: This method is common in practice but offers limited guarantees. Young people can easily circumvent this requirement by providing a false declaration.

Age verification: Using identity documents or other authoritative references (such as a bank account), the user's age is confirmed by an authorising body.

In theory, new app infrastructures could be developed to support highly privacy-friendly and reliable verification processes. However, this infrastructure requires further development and is not yet ready for use in the Netherlands.

A general verification requirement may also impose disproportionate costs by making participation mandatory for all users, and may unjustly exclude vulnerable groups from participation.

Circumvention by young people remains possible, particularly by enlisting the help of adults and/or through the use of VPNs.

Age estimation: Platforms can estimate a user's age, for example based on user profiling (*age inference*) and/or biometric facial scans (*age estimation*).

Estimates are less reliable than verification and lead to more errors; both in admitting minors and in wrongly excluding adults. Circumvention remains possible in several ways. Depending on the implementation details, privacy risks can be significant.

In Australia, the first country to introduce a statutory minimum age for social media, a hybrid approach has been adopted, with age estimation as the starting point. Face scans and verification are only used in cases of doubt and during appeal procedures (successive validation, or the 'waterfall method').

Early figures from Australia point to limited compliance: a majority of young people aged 14 to 15 (around 63%) remain active on social media. Moreover, among those young people who have stopped using social media, **social norms** appear to play a relatively significant role: since the rules came into force, more than half of the deactivations are said not to have been carried out by the platform, but voluntarily by parents and/or the minors themselves. Future prospects remain uncertain: on the one hand, the regulator has identified several areas for improvement in the current implementation by platforms. On the other hand, it remains unclear whether social norms regarding compliance will strengthen or weaken in the future.

We consider a universal verification requirement for all social media users to be disproportionate. Such a requirement would entail significant implementation costs, as well as risks and restrictions in terms of fundamental rights for a large group of users, including the risk of exclusion for various vulnerable groups. And despite these costs, circumvention would still be relatively straightforward, for example through the use of VPNs or with the assistance of adults.

0.1.3 Other policy considerations

In addition to age assurance standards, there are other policy options available that affect the feasibility, effectiveness and proportionality of the minimum age.

Which social media platforms are 'insufficiently safe'? The coalition agreement aims for a minimum age 'as long as social media are insufficiently safe'. This phrasing could imply that all social media are now deemed categorically insufficiently safe for children. A **categorical approach** can contribute to legal certainty and enforceability in the short term. Conversely, the minimum age could also focus on particular social media services that are considered insufficiently safe. Such a **risk-based approach** helps to ensure proportionality, and thus reduces the likelihood of challenges on the grounds of fundamental rights.

Binary age limit or a tiered approach? The minimum age could be a single binary age limit (15 years), but could also be introduced in tiers with different rights for each age category (for example: a total ban up to the age of 13; restricted access subject to parental consent, time limits and/or a modified version of the service between 13 and 15). A tiered approach helps to ensure proportionality and enables young people to be introduced to social media under safer conditions. A potential drawback is that age estimation may become more challenging, as a finer distinction is required.

Role of parental consent: Minimum age limits (and other protective measures, such as usage time limits) may apply universally, or instead allow exceptions with parental consent. This too can help to preserve proportionality, and could, for example, serve as an intermediate solution in the context of a phased age limit and/or the regulation of 'safe' social media. However, the practical implementation of parental

consent is complex and may, depending on the technical implementation, pose privacy risks. Relying on parents may also exacerbate inequality and worsen the position of vulnerable groups.

Focus on high-risk services (pornography, gambling): Strict minimum age limits already apply to some services, which are rarely or never checked by providers: notably pornography platforms, but also gambling platforms, for example. Reforms that would now enforce strict age assurance on social media, without imposing at least the equivalent requirements on these high-risk services, could lose credibility and proportionality.

Expectation management and social norms: In every scenario, a significant level of non-compliance is to be expected. If a minimum age is introduced, expectation management is therefore appropriate, at least in the short term. Appealing to young people's sense of social responsibility, and involving and supporting parents and other stakeholders such as schools, can also help to encourage the highest possible level of compliance with a minimum age.

Contents

1 Introduction

1.1 Background

On 10 December 2025, Australia's first statutory minimum age for social media came into force.[3] More and more countries are now following suit. France, Spain, Greece, Denmark, the UK and countless other countries have now announced similar policy intentions. In a relatively short space of time, the minimum age for social media has become a central issue in policy discussions regarding the protection of children online.

This development reflects growing public dissatisfaction with the impact of social media on young people, and mounting concerns about the health and safety risks to this group. Increasingly, governments view a minimum age as a potentially necessary tool to protect children's welfare, and as a means to fulfil the duty of care for children's health and safety as laid down in (among others) the UN Convention on the Rights of the Child.

In the Netherlands, the new coalition agreement of 30 January 2026 expresses the same ambition: 'An enforceable European minimum age of 15 for social media with privacy-friendly age verification for young people, as long as social media are not sufficiently safe'.[4] As grounds, the coalition agreement cites, among others, 'addictive algorithms, harmful content, and inadequate moderation' which contribute to 'addiction, bullying, abuse and fraud'.[5] State Secretary Willemijn Aerdts refers to the minimum age for social media as a measure for 'a safer and fairer digital environment, certainly for young people'.[6]

However, the legal implications of this policy are complex. Child protection in online services is already regulated at European level by laws including (among others) the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). A proposal for a new Digital Fairness Act (DFA) is also expected by the end of 2026, which may also include additional rules on child protection and safety by design. Fundamental rights and human rights also play a major role in the obligations of online platforms, including those towards children.

In view of these existing and forthcoming safety rules, the question arises as to whether, and to what extent, a minimum age can form a necessary and appropriate addition to the existing framework. Furthermore, important policy choices remain open regarding the age limit, such as the method of age verification and the scope of the ban on various platform services. Which policy choices and legislative route are most suitable for the Netherlands when introducing a minimum age, whether at EU level or at national level, therefore requires further investigation.

3 Ritchie, H., 29 November 2024. Australia approves social media ban on under-16s. BBC News.https://www.bbc.com/news/articles/c89vjj0lxx9o
4 https://www.kabinetsformatie2025.nl/documenten/2026/01/30/aan-de-slag---coalitieakkoord-2026-2030
5 Ibid.
6 https://www.linkedin.com/posts/stasdigi_twee-dagen-in-brussel-en-parijs-om-kennis-activity-7442479563273728000-vEl0

1.2 Main question and research plan

Against this background, this study addresses the following question:

> **"How can the objective set out in the coalition agreement regarding a European minimum age of 15 for social media be given legal effect?"**

For this project, we primarily employ a legal-doctrinal research method, with an emphasis on the systematic study and interpretation of legal sources such as legislation, regulations and case law. We have also conducted background interviews with several experts on topics including child protection and platform regulation. In addition, there is a comparative law component, insofar as we examine regulations from legal systems outside the Netherlands (chiefly: France and Australia). Where relevant, interdisciplinary insights from the social sciences are also incorporated, for example regarding the safety risks for young people on social media and the effectiveness of age verification technologies. The analysis consists of three parts:

Legal framework (Chapter II): *How is online child protection regulated by existing legislation and regulations, and what gaps does this framework leave for a new age limit policy?*

Through a discussion of the applicable law, we identify the obligations online services already have regarding the protection of children, and their current duties concerning minimum ages and age verification. Based on existing literature, we also discuss the main challenges regarding effectiveness and enforcement. In doing so, we analyse the DSA, the AVMSD, the GDPR, the DFA, and fundamental rights and the rights of the child.

International comparison (Chapter III): *How have other governments designed an age limit, and to what extent has this policy proved effective?*

In this section, two international precedents for a minimum age are analysed in detail: (1) the Australian Social Media Minimum Age Bill, which has now come into force and helps to shed light on age assurance practices, and (2) the French proposal for a minimum age, which highlights the relationship between EU law and national law.

Scenarios and recommendations (Chapter IV): *By what legal means, and with what advantages and disadvantages, can the Dutch government introduce an age limit?*

Finally, there is a discussion of the legal options for a minimum age. Based on the preceding examples, we discuss policy considerations regarding the legal anchoring of key concepts from the coalition agreement, such as 'insufficiently safe' and 'social media', as well as possible alternative concepts. On this basis, a number of recommendations and policy choices are formulated. We then discuss the following three legislative scenarios:

- Enforcement of existing EU legal frameworks
- Legislation at national level with European enforcement
- Legislative amendment Legislation at EU level.

These scenarios focus on options available to the Dutch government (as opposed to the European Commission or supervisory authorities). The assessment emphasises proportionality, effectiveness and enforceability, with a discussion of the pros and cons from a policy perspective and within the context of EU and fundamental rights frameworks.

2 Legal framework

The protection of minors in the digital environment is regulated in Europe by various forms of legislation and regulations. Minimum age limits are also part of this toolkit. Under certain circumstances, as will become apparent, platforms in general, and social media in particular, are also bound by such minimum age limits. In addition to minimum ages, EU law provides for many other methods of protecting children, with the emphasis not on prohibiting use by minors, but on improving their experience on these services. The law also sets limits on the enforcement of minimum ages by imposing conditions for the protection of privacy and other fundamental rights

The key obligations in this area stem from the relatively new Digital Services Act (DSA). Following an in-depth discussion of this framework, the Audiovisual Media Services Directive (AVMSD) and the General Data Protection Regulation (GDPR) will also be examined. Finally, fundamental rights will be addressed, with a focus on the rights of the child.

2.1 Digital Services Act (DSA)

2.1.1 Introduction

The DSA is the new cornerstone of EU platform law, which came into full force on 17 February 2024.[7] The DSA contains a range of rules on, among other topics, moderation procedures, ad targeting and recommender systems. No explicit minimum age for social media or other services is specified. However, there are general frameworks for the protection of minors which, depending on the circumstances of the case, may also require a minimum age. The key provisions are laid down in Article 28 on the Online Protection of Minors. The broader framework on systemic risks (Articles 34 and 35) is also relevant.

The DSA rules apply to intermediary services, including online platforms and search engines. Online platforms are, in short, internet services which, at the request of a user of the service, store and disseminate information to the public.[8] This broad category therefore includes social media platforms such as Snap, Instagram and YouTube, but also e-commerce services such as Zalando and Airbnb; app stores such as Google Play; and pornography platforms such as Pornhub.

For very large online platforms, with more than 45 million users, additional obligations regarding systemic risks (Articles 34–35 DSA) apply, which are also relevant to child protection. Furthermore, a different supervisory framework applies: very large online platforms and search engines are supervised primarily by the European Commission.[9] Smaller platforms are supervised by the national supervisory authority ('Digital Services Coordinator') of the place of establishment – in the Netherlands, the Netherlands Authority for Consumers and Markets (ACM).[10]

7 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act, hereinafter 'DSA')

8 DSA, Article 3(i). Excluded are cases where the storage and publication of user activity "minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation."

9 DSA, Article 56(2)-(4). For these major services, the Digital Services Coordinator of the place of establishment has only supplementary competence.

The very large platforms and search engines under supervision by the European Commission are:[11]

AliExpress	YouTube	TikTok
Amazon	Shein	X
Apple App Store	LinkedIn	Temu
Pornhub	Facebook	XVideos
Booking.com	Instagram	WhatsApp
Google Search	Bing	Wikipedia
Google Play	XNXX	Zalando
Google Maps	Pinterest	
Google Shopping	Stripchat	

2.1.2 Key obligations

The Protection of Minors under Article 28 of the DSA stipulates that online platforms accessible to minors must take 'appropriate and proportionate measures' 'to ensure a high level of privacy, safety and security of minors within their service'.[12] This very general principle is further elaborated in the preamble to the DSA and in Guidelines published by the European Commission on 10 October 2025.[13]

An online platform is likely to be 'accessible to minors' in the sense of Article 28 DSA; this applies not only to services used primarily by minors, but also to services where the provider is aware that some of its users are minors.[14] However, the precise responsibilities imposed by Article 28 DSA vary by service, depending on the specific risks involved. This risk assessment is further explained in the Guidelines on measures to ensure a high level of privacy, safety and security for minors online, published by the European Commission on 10 October 2025 (hereinafter: 'the Guidelines').

Under the DSA, the European Commission is empowered to draw up such Guidelines to assist providers in applying the child protection rules set out in Article 28(1) of the DSA.[15] These Guidelines thus reflect an authoritative interpretation of the DSA. Nevertheless, the final say on matters of interpretation rests with the Court of Justice of the European Union (CJEU). The Guidelines have not yet been reviewed by the CJEU or by other courts. A degree of uncertainty therefore remains. In any event, the Guidelines offer the most detailed and authoritative interpretation of Article 28 of the DSA that is currently available. Below, we first discuss the general principles of risk assessment, followed by their application to age verification and social media.

10 DSA, Article 56(1). The Digital Services Coordinator may also share certain powers with other national authorities (DSA, Article 49).
11 https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses. Some of these services (AliExpress, Booking.com, Snapchat, Wikipedia) are established in the Netherlands and are therefore subject to supplementary supervision by the ACM.
12 DSA, Article 28(1).
13 Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 (C/2025/5519). Communication from the European Commission. ('The Guidelines')https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:C_202505519.
14 DSA, para. 71.
15 DSA, Article 28(4).

Guidelines: Risk Assessment

The Guidelines do not require uniform measures from all online platforms; rather, the appropriate measures must take into account the specific context of the service on the basis of a risk assessment.[16] This assessment must take into account:

> (a) how likely it is that minors will have access to the service;
> (b) the likely impact of the service on the privacy, safety and security of minors;
> (c) the measures the provider is already taking to prevent and mitigate these risks;
> (d) any additional measures that providers may need to take;
> (e) how the measures ensure compliance with the general principles of [Section 4 of the Guidelines];
> (f) the parameters the provider uses to monitor, in the long term, the effectiveness of the measures it has taken to address certain risks; and
> (g) the potential positive and negative consequences for children's rights.[17]

In carrying out this assessment, platforms must also take into account, amongst other things, "the most up-to-date information and insight available from scientific and academic sources".[18] This assessment must be carried out at least once a year, and must subsequently be made available to the relevant supervisory authorities and published (with commercially sensitive information redacted).[19] To assist with this, platforms may also make use of existing frameworks, including the Dutch Ministry of the Interior and Kingdom Relations' Child Rights Impact Assessment.[20]

For very large platforms, this risk assessment may also be carried out as part of the general assessment of systemic risks in accordance with Article 34 of the DSA (discussed below).[21]

Thus, the obligations of platforms under the DSA vary depending on the nature of the service and the risks it poses to minors. For example, a distinction can be made between high-risk services that are inherently unsuitable for minors (pornography platforms or gambling platforms); general services on which minors are active (e-commerce and social media); and services specifically targeted at minors (certain educational and gaming platforms).

Guidelines: Rules on minimum ages

Under the current DSA framework, setting a minimum age is considered one possible measure to protect minors. The Guidelines emphasise that the minimum age is a supplementary tool, in the sense that it is not sufficient as the sole measure to protect minors.[22]

Platforms may also subject certain functionalities or content within their service to a minimum age—not just the entire service.[23] Conversely, providers may also set a maximum age to make certain platform services or functionalities accessible exclusively to minors.

---

16 Guidelines, para. 18.
17 Guidelines, para. 19.
18 Guidelines, para. 20.
19 Guidelines, para. 21.
20 Guidelines, para. 22.
21 Guidelines, para. 23.
22 Guidelines, para. 31. ("In this regard, the Commission is of the view that providers should consider access restrictions based on age, supported by age assurance measures as a complementary tool to measures set out in other sections of these guidelines. In other words, access restrictions and age assurance alone cannot be substitutes for measures recommended elsewhere in these guidelines.").
23 Guidelines, para. 36.

A minimum age can be enforced by means of various age assurance techniques; which technique is deemed legally appropriate again depends on the circumstances of the case (explained in more detail below).

The Guidelines identify three general categories of age assurance techniques:

- Self-declaration by the user
- Age estimation (based on behavioural information and other user data)
- Age verification (based on physical identification methods or verified identification sources).

Age verification is, in principle, the most accurate and reliable assurance method, but it can also have a greater impact on the privacy, data protection and other fundamental rights of data subjects.[24] Self-declaration by the user, on the other hand, poses limited privacy risks but is generally ineffective; the European Commission hence does not consider it an appropriate measure under Article 28 of the DSA.[25] Age estimation is a middle ground that is more effective and intrusive than self-declaration but, depending on the precise implementation, is generally less intrusive and effective than age verification.[26]

According to the Guidelines, a minimum age supported by age verification is an appropriate measure for services posing a high risk to minors, where these risks cannot be mitigated by less restrictive measures. This category includes, in any event, services aimed at (1) the sale of nicotine products and drugs; and access to (2) pornographic content and (3) gambling content.

For social media, the Guidelines are less clear-cut. Unlike the previous categories, the European Commission does not appear to conclude that social media are inherently so risky that a minimum age or age verification is always necessary. The starting point is therefore an assessment of the specific circumstances of the case; should research demonstrate that a social media platform poses specific risks to minors, which are not or insufficiently mitigated by other protective measures, then age-restriction measures may be required.[27] It remains unclear, however, exactly what evidence would be required to justify this conclusion. What is certain, however, is that age verification is not mandatory a priori for all social media.

An important addition is that, according to the Guidelines, national legislation may indeed impose a minimum age for social media. In this case, the platform is obliged to apply age verification:

> *"where Union or national law, in compliance with Union law, prescribes a minimum age to access certain products or services offered and/or displayed in any way on an online platform, including specifically defined categories of online social media services".*[28]

In other words: national and EU legislators may stipulate that a minimum age applies to certain platform services, including (specifically defined categories of) social media. In this way, the Guidelines also anticipate national legislation, such as that of France and Spain, which seeks to introduce a minimum age (see Chapter III.2).[29] Following the introduction of these laws, the platforms in question will also be under

24 See, however, the comment in the Guidelines, para. 33: "The Commission notes that a lower accuracy of age estimation solutions does not automatically equate to a lower impact on the fundamental rights and freedoms of recipients, as less accurate solutions may process more personal data than more accurate ones."
25 Guidelines, para. 52.
26 See, however, footnote 24 above. The premise that age estimation is more proportionate than verification is also contested by independent experts. See: Shaffique, M. & van der Hof, S., 2026. Behavioural profiling for age assurance: do the ends justify the means?, International Data Privacy Law, 16(1),https://doi.org/10.1093/idpl/ipaf012.
27 Guidelines, para. 37(c).
28 Guidelines, para. 37(d).
29 The Guidelines do state that such national legislation must be 'in accordance with Union law'. In Chapter III, we discuss the possible limits based on the French example. Furthermore, the Guidelines indicate that the TRIS notification procedure under Directive (EU) 2015/1535 applies. Guidelines, para. 37(d) footnote 37.

an obligation under the DSA to implement adequate age assurance techniques, so that illegal access by minors is effectively prevented.

In summary, an obligation to verify age for social media is not explicitly laid down in the Guidelines based on Article 28 of the DSA, but may apply in two cases: (a) where another national or EU law prescribes it, or (b) where the risk assessment in accordance with the Guidelines indicates that risks to minors for a particular service cannot be mitigated by other, less restrictive measures.[30]

In other cases, age estimation is considered more appropriate: (a) if the terms and conditions of a service impose a contractual minimum age of under 18 , or (b) where medium risks have been identified in the risk assessment, and those risks cannot be mitigated by less restrictive measures.[31] Age estimation may also serve as an alternative measure for higher-risk services, as long as no suitable age verification technology is available, either as a supplement or as a temporary measure.[32] A further discussion of various age estimation techniques and best practices follows in Chapter III.1, in the context of the Australian minimum age law.

Guidelines: Age assurance techniques and safeguards

The Guidelines also set out certain requirements for age assurance. Assurance measures must, first and foremost, be effective, in the sense that they are accurate and not easily circumvented. There are also standards in place to safeguard privacy, in accordance with the legal requirement under Article 28(3) of the DSA that "[c]ompliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor." This is a significant limitation on the possibilities for enforcing age verification under the current framework, particularly for age estimation, which also appears to go further than the standards set out in the GDPR (see Chapter II.3 below).

The Guidelines reiterate that age verification cannot serve as a licence for platforms to process even more data about their users: "Age verification should not entitle providers of online platforms to store personal data beyond information about the user's age group."[33] This wording does, however, appear to deviate from the legal standard set out in Article 28(3) of the DSA.[34] Regardless of these subtle differences, however, it is clear that there are tensions between age verification techniques and the need to limit data collection (to what is strictly necessary). The European Commission sees a solution in cryptographic applications, whereby ID card data or other forms of identification are verified not by the platform but by

30 According to the structure of the Guidelines, these requirements are alternative, not cumulative (see para. 37). A minimum age may derive either from national legislation or from the risk assessment based on the Guidelines. Nevertheless, national legislation must also comply with similar requirements of subsidiarity; in the national legislative context, a requirement of subsidiarity follows from the constitutional frameworks, not from Article 28 of the DSA. In concrete terms, this means that the national legislator, whilst bound by constitutional frameworks of necessity, proportionality and subsidiarity, is not obliged to carry out the full risk assessment under Article 28 of the DSA before prescribing a minimum age. For example, this leaves scope to give greater weight to the precautionary principle (for instance, by applying the minimum age categorically to all social media, rather than carrying out an assessment for each service).

31 Guidelines, para. 47.

32 Guidelines, para. 39.

33 Guidelines, para. 39.

34 Firstly, the emphasis here is on storage, whereas Article 28(3) refers to processing – a broader concept that encompasses not only storage but also collection, organisation, transmission, alteration, retrieval, use, erasure and more. Secondly, the standard is worded differently; the Guidelines describe a lack of legal basis ('should not entitle … to store'), whereas Article 28(3) concerns a restriction on the obligation to verify ('shall not … oblige to process'). This distinction may be relevant, as age verification may make use of data that platforms already collect and store for other purposes (for example: registration date, IP address, and so on – see Chapter III.1 for a further discussion). Under the Guidelines, it appears possible that Article 28 DSA may, under certain circumstances, oblige platforms to further process data already collected for the purposes of age verification. However, based on a stricter, literal interpretation of Article 28(3) of the DSA, it can be argued that platforms are not obliged to use this data for age verification — in other words, that the DSA cannot oblige platforms to process additional data for age verification, apart from the age of majority itself. However, this strict interpretation would render many age verification techniques, including many forms of age estimation, impossible. This does not appear to be the intention of Article 28(3) of the DSA, which seems simply to aim to prevent Article 28 of the DSA from acting as a licence for platforms to expand their surveillance of users even further. The interpretation set out in the Guidelines reflects this intention.

an independent third party.[35] The platform receives only an anonymised age token, which confirms the user's age but does not convey any additional information (such as, for example, the details in a passport copy). The European Commission encourages double-blind anonymity in this context: the platform receives no additional data on the user's identity (apart from confirmation of legal age), and the trusted third party does not know for which platform service the age verification is being used.[36]

An infrastructure for age verification by independent third parties is currently under development. For the longer term, a European Digital Identity Wallet is being developed, which will also be usable for age verification in due course.[37] To meet the requirements of the Guidelines in the shorter term, the European Commission has launched an initiative for an EU reference standard for age verification, also known as a 'white-label solution' or 'mini-wallet' (hereinafter: the EU Age Verification App).[38] This solution serves as a technical standard that can be integrated by public and private parties into their national identity infrastructures.

Pilot projects for the Age Verification App were launched in several Member States last year. Following this test phase, on 29 April 2026 the European Commission adopted a Recommendation stating that the standard is now ready for implementation, and urging Member States to make use of it.[39] An in-depth analysis of this app goes beyond the scope of this report, but it is worth noting that many experts have expressed criticism of this solution.[40] Any implementation in the Netherlands also raises new policy issues, including those concerning the participating authorities, the legal basis, and so on. Whether the EU reference standard will indeed offer a viable solution (in the short term) for the Dutch context therefore requires further consideration.

Online platforms and third parties are also free to develop their own verification solutions. However, in order to comply with the Guidelines, these solutions must be compatible with the aforementioned reference standard of the EC pilot project, which therefore effectively serves as a minimum standard. In theory, industry stakeholders may also develop their own standards in consultation with the Commission, in the form of a code of conduct under Article 44(1)(j) DSA.[41]

To conclude this section, the Guidelines set out an assessment framework for platforms to select an age verification technique, comprising: (a) accuracy, (b) reliability, (c) robustness, (d) non-intrusiveness, and (e) the prohibition of discrimination.[42]

35 Guidelines, para. 41.
36 Guidelines, para. 44.
37 Guidelines, para. 42. See also: Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework.
38 https://ageverification.dev/.
39 Commission Recommendation of 29 April 2026 on establishing a common framework for EU wide age verification technologies. C(2026) 4225 final.https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies.
40 Among others: Baum, C. et al., 2024. Cryptographers' Feedback on the EU Digital Identity's ARF. https://www.cs.ru.nl/~jhh/publications/cryptographers-feedback.pdf. Van Gend, T. 2026. Europe's Age Verification Push Raises Privacy Issues Beyond Data Confidentiality. Tech Policy Press. https://www.techpolicy.press/europes-age-verification-push-raises-privacy-issues-beyond-data-confidentiality/. Joint statement of security and privacy scientists and researchers on Age Assurance, 9 March 2026.https://csa-scientist-open-letter.org/ageverif-Feb2026. Soares, J., 2026. The EU's Age Verification Fix May Create More Problems Than it Solves. Tech Policy Press. www.techpolicy.press/the-eus-age-verification-fix-creates-more-problems-than-it-solves/. Castro, C. 2026. The EU's age verification app has a privacy problem — and it may be more than just a 'bug in an app'. TechRadar. https://www.techradar.com/vpn/vpn-privacy-security/the-eus-age-verification-app-has-a-privacy-problem-and-it-may-be-more-than-just-a-bug-in-an-app. (Note: Some of this criticism is directed at older versions of the app and is therefore not entirely up to date.)
41 Commission Recommendation of 29 April 2026 on establishing a common framework for EU-wide age verification technologies. C(2026) 4225 final. ("Finally, Article 44(1)(j) of Regulation (EU) 2022/2065 enables the Commission to support and promote the development and implementation of voluntary targeted standards to protect minors online. While no such standards have yet been developed, this could include technical standards for age assurance, including age verification").
42 The Guidelines, para. 49.

Guidelines: other protective measures

In addition to minimum ages, the Guidelines also discuss a range of other measures that platforms can take to protect minors. As mentioned, minimum age policies are regarded by the European Commission as a supplementary measure, and platforms are always expected to develop a broader child protection strategy. Such measures remain relevant after the introduction of a minimum age, at least to protect those minors who manage to circumvent age verification. As discussed in Chapter III.1, it is currently plausible that such circumvention will occur on a relatively large scale. The availability of alternative measures also plays a role in the assessment of the proportionality and subsidiarity of minimum age requirements, which are a relatively far-reaching measure.

In the Guidelines, the European Commission identifies a large number of measures that are either mandatory for all platforms accessible to minors, or are considered best practice and, depending on the nature of the service, may be regarded as appropriate measures. A detailed discussion of all possible measures is beyond the scope of this report, but in brief, the following measures are explored:

> **Account settings:** Accounts held by minors should be provided with secure settings in several ways. These security measures may apply to all known minor accounts and, furthermore, serve as the default setting for other accounts.[43] Among other things, platform settings should, by default , ensure that minors can only share content with, and interact with, accounts they have previously accepted into their network; that minors' activities (such as 'liking' posts) are not visible to third parties; that the default playback of videos and hosting of live streams is disabled; that access to device functions such as geolocation, microphone and camera is disabled; that push notifications are disabled during core sleeping hours; that recommendations from other accounts are disabled; and many other such measures.[44]
>
> **Availability of settings, features and functionalities:** The Guidelines stipulate that certain functionalities must never be available to minors, including: being easily found or contacted by accounts they have not previously accepted as contacts; disclosing the minor's personal contact details, such as an email address or telephone number, without explicit consent; and never including minors' accounts in account suggestions to adults.[45]
>
> **Design of online interfaces and other tools:** Measures to empower minors over their online environment are encouraged, including time management tools to make users more aware of the amount of time they spend on the platform.[46] However, design choices that are primarily aimed at engagement and that may lead to extremely high or excessive use of the platform, or to problematic or compulsive behaviour, should be avoided. These include, for example, infinite scroll, autoplay, and push notifications with manipulative timing or content.[47]
>
> **Recommender systems and search functions:** Platforms can take measures to ensure that recommender systems do not enable or facilitate the dissemination of illegal content or the commission of criminal offences against and by minors. In addition, they can ensure that search functions do not recommend content deemed harmful to the privacy, safety and/or security of minors, for example by blocking search terms known to lead to such content.[48] Minors can be referred to appropriate support resources and helplines if they have questions about such

43 Guidelines, para. 57(a) in conjunction with (b).
44 Ibid.
45 Guidelines, para. 59(b).
46 Guidelines, para. 61.
47 Guidelines, para. 61(b).
48 Guidelines, para. 65(k).

content.[49] Platforms can enable minors to completely and permanently reset their recommended feeds; regularly encourage minors to search for new content; and so on.

Tools for users and guardians: User tools can enable minors to block (among other things) unwanted content or contacts. Tools for parents can also play an important – though, like age verification, supplementary – role.[50] Platforms available to children should develop their own parental control options and be compatible with the range of interoperable third-party control tools ('one-stop-shop' tools).

The Guidelines also contain recommendations regarding commercial practices (including the prevention of the exploitation of minors through manipulative advertising practices) and moderation (including the removal or demoting of content harmful to minors), reporting (visible and child-friendly complaint mechanisms for harmful content, features, etc.) and governance (operational aspects such as monitoring, evaluation and transparency).

2.1.3 Articles 34 and 35 – Assessment and mitigation of systemic risks

Under the DSA, additional obligations apply to very large platforms with more than 45 million monthly users. The main obligations are to regularly assess (Article 34) and subsequently mitigate (Article 35) so-called systemic risks. This concept is very broad and has no explicit definition. The key principle underlying Article 34 is that, in any event, the following risks (non-exhaustive list) must be assessed: the dissemination of illegal content; negative effects for the protection of fundamental rights; serious negative consequences for a person's physical and mental well-being; and – most relevant to this report – the protection of minors.

Very large platforms and search engines must carry out an annual assessment of the specific risks arising from the use of their service. They must then take appropriate measures to mitigate these risks. These measures must be reasonable, proportionate and effective. Article 35 of the DSA provides a long, indicative list of possible measures, explicitly mentioning: "taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate".[51]

In practice, there appear to be few significant differences between the obligations of large platforms regarding child protection under Articles 34–35 DSA and Article 28 DSA. Both articles require a risk-based approach, in which the platform provider initially determines its own measures based on the specific risks associated with its service. Nuances in the wording ('targeted' or 'appropriate' measures, for example) do not indicate fundamentally different obligations. This conclusion appears to be shared by the European Commission ; as mentioned above, their Guidelines require the following of very large platforms:

> 23. For providers of [very large online platforms and search engines] this risk review can also be carried out as part of the general assessment of systemic risks under Article 34 of Regulation (EU) 2022/2065, which will complement and go beyond the risk review pursued in accordance with the present guidelines.[52]

The final clause also indicates that the obligations for very large platforms and search engines are stricter ('go beyond') than those for other, smaller services. Under the DSA's risk-based approach, larger services

49 Ibid.
50 Guidelines, para. 80.
51 DSA, Article 35(1)(J). For a further discussion of the rights of the child, see Chapter II.5.

are generally subject to more demanding obligations, given that they can have a greater societal impact.[53] Furthermore, larger services generally have more resources and expertise at their disposal to mitigate risks. When assessing the implementation of age verification measures under Articles 28 and 35, the size of the platform may therefore be taken into account. Depending on the specific circumstances of the case, it is conceivable that a minimum age or age verification obligations would apply to very large social media platforms under the DSA, but not to smaller services.

2.1.4 Country of origin principle and harmonising effect

Also relevant to this study is the country-of-origin principle, which limits Member States in their regulation of internet services in other Member States. This principle is one of the oldest cornerstones of EU internet law and is enshrined in the predecessor to the DSA: the Electronic Commerce Directive of 2000, also known as the 'e-Commerce Directive'.[54]

The aim is to facilitate the free movement of services and prevent fragmentation of the European market, which is of particular relevance for internet services that regularly operate across borders. The principle has come under pressure over time, as Member States have seen a greater need to regulate internet services. During the drafting of the DSA, there was extensive debate about the possible abolition or amendment of this principle, but ultimately it was retained. The key compromise in this area was to place oversight of very large platforms with the European Commission, in order to prevent a race to the bottom in enforcement among Member States.

There are exceptions to the country-of-origin principle for information society services. Member States may derogate from the principle if the measure is necessary to achieve certain objectives, including "the protection of minors".[55] Furthermore, the measure must be taken in respect of internet services "which prejudices the aforementioned objectives, or presents a serious and grave risk thereof". The measure must also be proportionate to that objective. It can therefore be argued that measures concerning child protection on social media may fall under this exception; however, a final assessment depends on the specific circumstances of the case. A Member State invoking this exception must notify the European Commission of its intention, so that the Commission can assess its compatibility with EU law.[56] It must also first request the Member State of establishment to take measures; its own measure is only permitted if the latter fails to respond or responds inadequately.

With the introduction of the DSA, the substantive obligations for internet services, particularly online platforms, have been further harmonised. As a result, the country of establishment is also restricted in the additional requirements it can impose on these services. As indicated above, the European Commission does note in its Guidelines that minimum age limits at national level may be compatible with the DSA. The practical application of these principles is discussed in more detail below in the French context (Chapter III.2) and the Dutch context (Chapter IV.2).

52 Guidelines, para. 23.

53 DSA, para. 76. ("Very large online platforms and very large online search engines may cause societal risks, different in scope and impact from those caused by smaller platforms. Providers of such very large online platforms and of very large online search engines should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact."). See also: De Gregorio, G.and Dunn,P., 2022.The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age.Common Market Law Review59(2) https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/59.2/COLA2022032.

54 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("e-Commerce Directive"), Article 3.

55 e-Commerce Directive, Art 3(4)(a). See also the recent analysis by Advocate General Szpunar on the French pornography measure 'SREN', with a strict interpretation of the relevant grounds for exemption: CJEU 18 September 2025 C-188/24, ECLI: EU:C:2025:709 Opinion of the Advocate General (Szpunar). Opinion of Advocate General (Szpunar) at the Court of Justice of the European Union 18 September 2025, ECLI:EU:C:2025:709.

56 e-Commerce Directive, Article 3(5) and (6).

2.1.5 Recent enforcement measures

In recent months, there have been many significant developments in the enforcement of the DSA in relation to specific services, in particular the rules on child protection and age verification. Some key developments are discussed below.[57]

Alleged DSA infringement due to TikTok's addictive design (6 February 2026)[58]

Summary: The European Commission has provisionally concluded TikTok did not adequately assess how these addictive features could harm the physical and mental wellbeing of its users, including minors and vulnerable adults. TikTok's mitigation measures, such as the screen time management and parental control tools it offers, do not appear to effectively reduce these risks. The European Commission believes that TikTok must make changes to the design of the service, including disabling addictive features such as 'infinite scroll', implementing effective 'screen time breaks', including at night, and revising the recommender system.

Relevance: This measure is not directly aimed at minimum age limits, but does explore other possibilities for safety by design (which are complementary to, or may serve as an alternative to, a minimum age limit).

Alleged DSA infringement due to inadequate age verification on pornography platforms (26 March 2026)[59]

Summary: The European Commission has provisionally determined that several major pornography platforms (Pornhub, Stripchat, XNXX and XVideos) are in breach of the DSA due to inadequate checks on user age. These platforms state in their terms and conditions that their services are intended solely for adults. However, use by minors is verified solely through self-declaration, which the European Commission considers inadequate. The European Commission also considers these platforms' risk assessments to be insufficient in terms of the protection of minors. In its view, these services must introduce privacy-preserving age verification.

Relevance: With this action, the European Commission has, for the first time, identified a breach of age verification obligations under the DSA. Principles from the Guidelines are being applied in a specific case: self-declaration is insufficient, and high-risk services such as pornography platforms must implement age verification.

Investigation into child protection at Snapchat (26 March 2026)[60]

Summary: By exposing minors to harmful content (grooming attempts, criminal recruitment, and the sale of illegal and age-restricted goods, including vapes), Snapchat may have breached the DSA. Snapchat's terms and conditions stipulate a minimum age of 13, and the European Commission suspects that this is not being adequately enforced, and that the current self-declarations are insufficient as a safeguard. A reporting function to flag underage accounts does not appear to be available. The investigation also focuses on measures to restrict harmful content

57 For each case, the most recent measure is discussed. For example, the announcement of the investigation into TikTok is not considered here, in favour of the final findings.
58 https://ec.europa.eu/commission/presscorner/detail/nl/ip_26_312.
59 https://ec.europa.eu/commission/presscorner/detail/en/ip_26_722.
60 https://ec.europa.eu/commission/presscorner/detail/en/ip_26_723.

Relevance: With this investigation, the European Commission is taking a first step towards enforcing minimum age limits for social media. The 13-year-old threshold is lower than that currently pursued by many governments, but it does correspond to industry standards and certain academic recommendations. With the emphasis on enforcing the platform's own contractual age limit in its terms of service, it remains unclear whether the European Commission would, under certain circumstances, also consider a minimum age to be mandatory as a restriction measure (and possibly even a higher age) for unsafe social media. In any case, this investigation is not yet complete; for the time being, no definitive conclusions can be drawn from it.

Alleged DSA infringement due to inadequate age verification on Meta platforms (29 April 2026)[61]

Summary: The European Commission has provisionally found Meta to be in breach of the DSA due to inadequate enforcement of the minimum age of 13, which is included in their terms and conditions. The self-declaration required when creating an account is easy to circumvent, and the reporting function for flagging underage accounts is difficult to use and often ineffective. Underlying this inadequate policy is an "incomplete and arbitrary risk assessment", which fails to take into account (among other things) the "large bodies of evidence from all over the European Union indicating that roughly 10-12% of children under 13 are accessing Instagram and/or Facebook".

Relevance: In terms of age verification, this case bears many similarities to the investigation into Snap; here too, the issue concerns a contractual minimum age of 13 for social media. What is significant about this case is that it is at a more advanced stage; whilst an investigation into Snap has only just been announced, the investigation into Meta has been ongoing for some time and preliminary findings have now been reached. Although Meta can still seek review of these findings, this case at least indicates that the European Commission considers itself capable of identifying breaches of age verification obligations on social media and taking enforcement action against them. At this stage, it is not yet clear which alternative age verification measures (verification or estimation) the European Commission considers appropriate. The general principles set out in the Guidelines remain the guiding principles here, and these point to estimation as the appropriate method where a contractual minimum age applies.

2.1.6 Discussion

In summary, the DSA already provides relatively detailed and ambitious rules regarding child protection on social media. A minimum age is among the possible measures, and standards for age verification technology are currently being developed.

A key principle of the DSA appears to be that platforms are, in any case, responsible for enforcing the age restrictions set out in their own terms and conditions. For social media, the standard minimum age is 13, but enforcement through self-declaration is generally subject to many limitations. Recently, the European Commission has taken steps to enforce stricter compliance with this contractual minimum age, including by taking enforcement action against Meta and Snap. In doing so, it suggests that both estimation and verification can be appropriate measures. With the new EU Age Verification App as a technical standard, Member States are now also encouraged to develop an age verification app that fits the national context. The privacy risks involved in age verification are explained in more detail in Chapters II.3 (on the GDPR) and II.5 (on fundamental rights).

61 https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920.

A follow-up question is whether the DSA itself imposes a statutory minimum age for social media, which may be higher than the contractual age. The DSA is less explicit on this point, and a specific risk assessment for each service remains the guiding principle. There is therefore no categorical minimum age that is directly enforceable for all social media, but rather a standard that may apply to certain unsafe social media platforms. It can therefore be argued that the DSA already complies with (a certain interpretation of the coalition agreement) as a framework for a minimum age for 'insufficiently safe' social media; albeit in a less categorical manner than some might expect. (It is worth noting that the European Commission's most significant enforcement actions also date from after the coalition agreement.) Chapter 4 weighs up the benefits of the risk-based approach under the DSA against a more categorical approach, whereby the minimum age would apply to all social media platforms.

The DSA also offers a multitude of other protective measures for minors, which emphasise improving the user experience. Here too, enforcement is beginning to take shape, for example against TikTok's addictive algorithmic techniques. Experimentation with standards such as time locks and restrictions on infinite scroll points to potential opportunities to make social media safer for minors. It is important to reiterate that minimum ages under the DSA are only intended as a supplementary measure, and that an improved user experience takes priority at least in principle. It is not the intention that the minimum age should serve as a catch-all in policy and enforcement, thereby potentially preventing other important measures from being taken. This trade-off – between improving and banning social media among young people – is also discussed in more detail in Chapter 4.

2.2 Audiovisual Media Services Directive (AVMSD)

2.2.1 Introduction

The Audiovisual Media Services Directive (AVMSD) is primarily aimed at regulating television and streaming services with editorial content. Since a revision in 2018, it has also included provisions relevant to video platforms with user-generated content. Video platforms must protect minors from exposure to content that could harm their physical, mental or moral development.[62] Age verification may also form part of this responsibility.

Unlike the DSA, the AVMSD applies only to "video-sharing platform services". This category is not defined as a subcategory of "online platforms" under the DSA, but has its own definition; in short, it refers to services that make video content available without exercising editorial control over it, organised using, among other things, automated means or algorithms.[63] As they often offer video functionality, most social media platforms also fall under this definition and are therefore regulated by both the DSA and the AVMSD.

Supervision of this framework does not lie with the European Commission but with independent media supervisory authorities at national level. In the Netherlands, the Media Authority is responsible for supervising providers of video-platform services established in the Netherlands. Many video-platform services are established in Ireland, which means that the Irish authority, *Coimisiún na Meán*, plays a key role in supervising the AVMSD. The services Snapchat and Reddit fall under Dutch supervision.[64] Facebook, Instagram, YouTube, TikTok, LinkedIn, X, Udemy, Pinterest, and Tumblr fall under Irish supervision.[65] To coordinate (among other things) the supervision of the AVMSD, national authorities sit on the European Board for Media Services (formerly 'ERGA').[66] Member States not only monitor compliance but may also "impose measures that are more detailed or stricter than those referred to in paragraph 3 of this Article".

62 AVMSD, 28b(1).

63 AVMSD, Article 1(1)(a). ("'video-sharing platform service' means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing;")

64 https://www.cvdm.nl/sector/videoplatformdiensten/.

65 https://www.cnam.ie/industry-and-professionals/online-safety-framework/online-safety-code/register-of-designated-online-services/.

66 This change of name was introduced in the recent European Media Freedom Act (EMFA). See: Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU.

2.2.2 Key obligations

The main child protection rule for video-sharing platforms under the AVMSD, set out in Article 28b, states that Member States must require them to:

> …"protect minors from programmes, user-generated videos and audiovisual commercial communications that may impair their physical, mental or moral development in accordance with Article 6a(1);"[67]

To this end, video-sharing platform service providers must take "appropriate measures", depending on the specific risks to minors on their service.[68] Similar to the Guidelines under the DSA, this risk-based approach is supported by a long list of possible measures. The AVMSD mentions

- amending the terms and conditions;
- mechanisms for reporting content to the provider;
- age verification systems for users of video platforms;
- parental control systems;
- procedures for complaints regarding the implementation of other measures;
- measures and tools in the field of media literacy.[69]

> This obligation applies to content for which media providers themselves also have obligations to prevent access by minors and to provide warning information via systems such as the Kijkwijzer (see Article 6a). The information provided by these providers can then be used by platforms to restrict access by minors and/or subject it to *parental controls.* The obligations under Article 28b may be further elaborated in codes of conduct, drawn up by industry stakeholders in consultation with the regulator ('co-regulation').[70]

No general code of conduct has yet been agreed in the Netherlands. In any case, the most significant developments are taking place in Ireland, where many of the major video platforms are based. The Irish media regulator, *Coimisiún na Meán* (CnaM), oversees (in addition to the DSA) the AVMSD and, in this context, published an Online Safety Code in October 2024. Under this Code, video platforms are obliged to implement effective *age assurance* if their terms and conditions do not include a ban on pornographic and extremely violent content.[71] The Code does not express a preference regarding the possible standards or techniques for age assurance, except that these must be 'effective' and that a single self-declaration by the user is, in any case, insufficient.[72] A separate Guidance document lists several options; in addition to the already familiar self-declaration, age estimation and verification, it also mentions alternatives such as cross-platform authentication (where verification is taken over from another, trusted platform), account holder confirmation (confirmation by another, already verified user) and capacity-testing (assessing users through puzzles or language proficiency tests).[73] However, the Guidance reiterates that CnaM does not take a position in advance on the suitability of these methods.[74]

---

67 AVMSD, Article 28b(1).
68 AVMSD, Article 28b(3). This provision also provides further clarification on the nature of this risk assessment: "For the purposes of paragraphs 1 and 2, the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest."
69 AVMSD, Article 28b(3).
70 AVMSD, Article 28b(9) in conjunction with Article 4a.
71 https://www.cnam.ie/industry-and-professionals/online-safety-framework/online-safety-code/.
72 Ibid.
73 https://www.cnam.ie/app/uploads/2024/11/Online-Safety-Guidance-Materials.pdf.
74 Ibid. ("[t]he Commission does not specify the method or methods by which platforms must verify or estimate the age of their users for the purposes required under the Code. The Commission recognises that a number of solutions may be possible".)

Since the requirements are focused on services that permit pornography and extreme violence, most social media platforms remain unaffected. Platforms including TikTok, Instagram and Facebook have such a ban in place. Exceptions are X and Reddit, which do permit pornography. Action has already been taken against X: in June 2025, CnaM established that X does not carry out age assurance, and ordered the platform to take measures or face a fine.[75]

The Online Safety Code also implements other child protection measures from the AVMSD, such as options for content rating by uploaders (allowing them to recommend or advise against suitability for children), alcohol advertising, measures to promote media literacy, and mechanisms for parental control. Parental control tools should enable parents of children under the age of 16 to protect their children from harmful content ("content… which may impair the physical, mental or moral development of children") and to restrict access to certain types of content (such as content from unknown users, or based on certain metadata).

Of course, the Code remains merely an interpretation of the applicable Irish and European law. A court, or the Dutch supervisor, might interpret the AVMSD rules on child protection differently. However, the Code remains highly relevant to current practice, because many major platforms are subject to Irish supervision. By emphasising pornographic content, and by leaving the choice of safeguard measures open in principle, the Online Safety Code is less stringent than the Guidelines under the DSA with regard to minimum ages.

2.2.3 Relationship with the DSA

Although they use different definitions, there is clear overlap between the DSA and the AVMSD when it comes to the protection of children. In practice, every video-sharing platform regulated by CnaM under the AVMSD is also an online platform under the DSA. Which framework takes precedence? In legal terms, these frameworks are likely to be very similar, in the sense that they both require 'appropriate measures' in line with the specific risks associated with the service. However, there are significant differences in terms of enforcement, which will fall to different supervisory authorities.

In 2025, the European Commission published an analysis setting out the relationship between the DSA, the AVMSD and other frameworks. It considers these frameworks to be complementary, and video platforms must, in principle, comply with both; compliance with the AVMSD does not therefore exempt video platforms from the obligation to comply with the DSA.[76] Where there is an overlap between specific obligations under the DSA and the AVMSD, the European Commission states that a case-by-case assessment must be made to determine which framework takes precedence. The European Commission regards the rules of the AVMSD and the DSA as complementary, and platforms must comply with them 'in parallel'.[77] Article 2(4) of the DSA makes it clear that it 'shall not affect' the AVMSD and certain other legislation. Consequently, the DSA must not 'amend these prior rules incidentally or unintentionally', but remains applicable to matters not addressed, or not fully addressed, by them. It is also relevant here that

75 https://www.cnam.ie/coimisiun-na-mean-issues-statutory-information-notice-to-x/.
76 Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts, SWD/2025/368 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025SC0368.
77 Ibid.

the DSA entails maximum harmonisation, whereas the AVMSD entails only minimum harmonisation.[78] Consequently, the DSA takes precedence on issues where it imposes more specific rules ("the DSA prevails where its harmonised and directly enforceable obligations are more specific"), including in the management of systemic risks and the risk mitigation measures to protect minors.[79] In practice, however, there does not appear to be a direct legal conflict between Article 28 of the DSA and Article 28b of the AVMSD, and it can be concluded that the two frameworks can coexist.[80] Naturally, this interpretation is not yet binding, and the Court of Justice of the European Union could potentially develop a different interpretation of its own.

Where both frameworks must be complied with simultaneously, the measure requiring the highest level of protection applies in practice. If, for example, CnaM were to conclude under the AVMSD that a minimum age of at least 16 is appropriate, and the European Commission were to set a minimum age of 15 under the DSA, the lower, stricter age would apply.

The differences in enforcement are significant. Enforcement of the AVMSD takes place at national level, whereas the DSA is, in many respects, also enforced at European level by the European Commission. Furthermore, enforcement of the AVMSD in the Netherlands falls under the remit of the media authority (*Commissariaat voor de Media*), whilst enforcement of the DSA falls primarily under the remit of the ACM. For platform services with their principal place of business in Ireland, CnaM is competent for both the AVMSD and the DSA.

2.2.4 Discussion

In summary, the child protection rules set out in the AVMSD do not differ hugely in substance from those in the DSA. Both contain a general obligation for platform services to take appropriate measures, depending on the specific risks associated with their service. Although the AVMSD was initially more detailed, the Guidelines have now further elaborated on the DSA. Through the Online Safety Code, the Irish supervisory authority, which plays a key role under the AVMSD, has adopted a relatively cautious interpretation of minimum age requirements compared to the Guidelines under the DSA. This approach focuses primarily on platforms that permit pornography and severe violence on their service.

The differences in scope and enforcement framework are significant. The AVMSD applies only to video-sharing platforms, whereas the DSA applies to online platforms in a broader sense. Furthermore, supervision lies with different authorities, and the DSA framework is considerably more harmonised, partly due to the important role of the European Commission as a supervisory authority. As explained in more detail in Chapter IV, this makes the DSA, in principle, a more attractive framework for implementing a (European) minimum age.

78 Ibid. (Further explained: "Article 2(4) clarifies that the DSA is "without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing this Regulation," followed by an explicit, non-exhaustive list of key legal acts. This "without prejudice" provision is fundamental, as it ensures that the DSA does not override or diminish the application of sectoral or horizontal rules in these areas. However, it is important to recognize that Article 2(4) DSA does not mean that the EU legal acts referenced in the list automatically are carved out from the DSA. Rather, the DSA remains a maximum harmonisation instrument that only gives precedence to provisions in other instruments that regulate other aspects of the provision of intermediary services (i.e., aspects not already harmonized by the DSA), or that provide additional or complementary obligations.")

79 Ibid.

80 Ibid. ("Both pieces of legislation are complementary and apply in parallel. […] Consequently, compliance with the AVMSD does not exempt such VLOPs from these DSA obligations.")

2.3 General Data Protection Regulation (GDPR)

The General Data Protection Regulation ('GDPR') regulates the processing of personal data and is therefore primarily aimed at protecting privacy, and in particular the fundamental right to the protection of personal data.[81] This general framework applies, with some exceptions, to the entire private and public sectors. The interests of children are further protected by the GDPR through specific provisions governing the granting of consent for the processing of minors' user data by online services. In addition, the GDPR also sets standards for protective measures such as age verification and age estimation. This chapter first discusses the rules on consent for minors, and then the processing of personal data where age is verified.

2.3.1 Consent of children in relation to online services (Article 8)

Legal bases for processing: consent and alternatives

Under the GDPR, a valid processing ground is required for the processing of personal data. One of these grounds is consent. Furthermore, valid consent under the GDPR must be freely given, specific, informed and unambiguous.[82]

For social media, where the business model relies on the large-scale processing of user data, consent is a very important processing ground. In practice, platforms also rely on alternatives, in particular the performance of a contractual obligation and the legitimate interests of the controller. However, supervisory authorities, including the EDPB, have concluded that these alternative bases are less far-reaching in terms of the amount and type of data processing they justify. The contractual obligation justifies data processing that is objectively necessary for the provision of the service (such as the storage of profile data and network relationships), but, according to the Court of Justice and the EDPB, cannot justify the additional processing of profiling that social media platforms carry out for commercial micro-targeting.[83] Consent therefore remains very important, though not entirely essential. Without valid consent, social media could, in theory, continue to offer a variant of their service, but this would require a radical change in their current processing practices and revenue model.

Parental consent for minors

The GDPR stipulates that online services (defined under EU law as 'information society services') may only rely on the data subject's consent if the data subject is at least 16 years old.[84] This rule therefore also applies to social media and other platform services.[85] For children under this age, consent is also required from the person who has parental responsibility for the child. Member States may deviate from this rule by introducing a lower minimum age, down to a lower limit of 13 years.[86] The Dutch implementation of the GDPR does not make use of this option, so the age limit for parental consent remains at 16 years.

---

81 Privacy is a key objective of the GDPR, but not its sole objective. Firstly, a distinction can be drawn between privacy and data protection as separate (yet overlapping) fundamental rights. Furthermore, the GDPR also serves to safeguard the exercise of other fundamental rights that may be at stake in the context of personal data processing, such as the right to dignity, freedom of expression and the prohibition of discrimination. See: Lynskey, O., 2014. Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. International & Comparative Law Quarterly, 63(3), pp.569-597.

82 GDPR, Recital 32.

83 EDPB (2024), Guidelines 8/2020 on the targeting of social media users (Version 2.0). CJEU C-252/21 4 July 2023 ECLI: EU:C:2023:537 (Bundeskartellamt). Under the DSA, it is already prohibited to process special categories of personal data relating to minors, such as political opinions or sexual orientation, in microtargeting; however, a lack of valid consent could therefore also exclude other, non-special categories of personal data. See: DSA, Article 28(2). See also: EDPB (2024), Guidelines 1/2024 on the processing of personal data based on Article 6(1)(f) of the GDPR.

84 Exception: No consent from parents or carers is required for preventive or counselling services offered directly and free of charge to children. See GDPR, Recital 38.

85 Online platforms are a subcategory of hosting services, and therefore a sub-subcategory of 'information society services', see DSA, Article 3.

86 GDPR, Article 8(1).

Article 8 of the GDPR applies only to services offered 'directly' to a child. According to the European Data Protection Board (EDPB), this is not the case if the provider makes it clear that the service is not intended for users under the age of 18 (and if this is not contradicted by the actual content or marketing of the service). For services that are directly offered to children, Article 8(2) imposes an obligation to make 'reasonable efforts' to verify parental consent.[87] For users who state that they are of legal age, the provider may also apply 'appropriate checks'.[88] The EDPB does not explicitly specify what these 'checks' would entail. Once again, a risk analysis applies, whereby less risky services may be able to suffice with a self-declaration. In other cases, 'alternative checks' may be considered, for example by requiring payment of a nominal amount (€0.01) or by collaborating with 'trusted third-party solutions'.[89]

These examples suggest that the parent's identity does not need to be established with absolute certainty. After all, the payment of a nominal fee can also be made by third parties of legal age. With this approach, circumvention remains possible, but privacy is also safeguarded. After all, definitively establishing a parental or guardianship relationship would require the processing of considerably more data. In this context, Article 11 of the GDPR is also relevant (although the EDPB does not mention it): compliance with the obligations under the GDPR cannot oblige controllers to process additional data for the sole purpose of identifying data subjects.[90] The EDPB's interpretation thus appears to accept a degree of uncertainty with the aim of preventing excessive data processing.

Parental consent in practice

In practice, Article 8 of the GDPR appears to have had a relatively modest impact. An empirical study by the civil society organisation Interface indicates that most major platforms take little or no measures to ensure parental consent.[91] It is also clear that providers generally do not rely on consent but on other legal bases; in particular, the fulfilment of a contractual obligation.[92] As discussed, however, it is doubtful whether this legal basis can justify all data processing by platforms (including commercial profiling that is not objectively necessary for the performance of the service).

However, a further complication is that minors may lack legal capacity, and there is no legally valid contract to serve as an alternative basis for processing. Legal capacity is a matter of national private law and therefore varies from one Member State to another, but a common principle in many legal systems is that minors lack legal capacity unless the acts in question are customary for their age.[93] Should a legally valid agreement indeed be lacking, then no alternative basis will be available apart from consent, and parental consent for minors becomes an absolute requirement. The processing of minors' user data without parental consent may therefore constitute a large-scale breach of the GDPR.

Platforms may potentially argue that they are unaware of these infringements; the GDPR does not impose explicit age verification obligations, and platforms can therefore argue that they are unaware of the unlawfulness.[94] A flaw in Article 8 of the GDPR is that it emphasises the duty of care when verifying

87 EDPB (2020), Guidelines 05/2020 on consent under Regulation 2016/679, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Hereinafter, "EDPB Guidelines 05/2020"): "Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR, it is implicitly required, for if a child gives consent whilst not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful."

88 EDPB Guidelines 05/2020, para. 133 ("If the user states that he/she is below the age of digital consent, the controller may accept this statement without further checks, but will need to proceed to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.")

89 EDPB Guidelines 05/2020, para. 137 and footnote 68.

90 GDPR, Article 11.

91 Jessica Galissaire (2025). Mind the Gap: Age Assurance and the Limits of Enforcement under EU Law. Interface. https://www.interface-eu.org/publications/age-assurance-gap.

92 Ibid.

93 Lynskey, O., 2014. Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. International & Comparative Law Quarterly, 63(3), pp.569-597.

94 EDP Guidelines 05/2020 ("Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.")

parental consent, but imposes relatively less stringent requirements on the *age verification* that determines when parental consent is required. However, a lack of knowledge is, in principle, no defence in this context; the controller itself has a duty to ensure a valid legal basis. However, the aforementioned Article 11 of the GDPR, which restricts additional data collection for the purposes of compliance with the GDPR, may also play a role in limiting age assurance obligations for social media in this context.

Interaction with the DSA

The DSA may provide an impetus for stricter enforcement of Article 8 of the GDPR. After all, the verification obligations under the DSA, for which enforcement is now being initiated, may oblige platforms to gain a better understanding of users' ages. And where a user's minority is known to the platform, they are also obliged under the GDPR to ensure parental consent. Recent DSA enforcement actions have focused on the contractual minimum age of 13, but under the GDPR, users are protected up to the age of 16 and parental consent is mandatory.[95]

In this (speculative) scenario, the GDPR and DSA could therefore operate in a complementary manner. However, this remains dependent on effective DSA enforcement, ensuring that platforms do indeed effectively verify the age of users. As discussed in Chapter II.1, only the first steps have been taken in this enforcement process. Furthermore, it appears that the GDPR supervisory authority may be exclusively competent for the enforcement of the consent rules under this Regulation.[96]

This division of supervisory tasks has clear drawbacks. Whilst the European Commission actively monitors the contractual minimum age on major platforms, it is not clear whether they can address the ongoing non-compliance with Article 8 of the GDPR and the rules on parental consent up to the age of 16. This is especially regrettable since, compared to data protection authorities, the European Commission's DSA enforcement team specialises in managing risks at the intersection of social media, safety and child protection. In Chapter 4, we discuss possible solutions.

2.3.2 Data protection in age assurance

In addition to regulating parental consent for internet services, the GDPR is also the primary regulatory framework for privacy risks associated with age verification. Below, we discuss the general principles of data protection law, followed by their application to age verification by the EDPB.

General principles

Age verification constitutes the processing of personal data and is therefore subject to the GDPR. This Regulation establishes a detailed and nuanced framework to ensure data processing is carried out properly. Some of the key requirements are discussed below: the general principles governing the processing of personal data; the requirement for a legitimate processing ground; and the additional protection for special categories of personal data.[97]

---

95 As discussed in the previous sub-chapter, there remains some legal uncertainty regarding the possibility of invoking the contractual obligation as an alternative legal basis. However, it follows from this analysis that parental consent is required in virtually every case involving minors in order to lawfully offer the service. This also depends on the geographical context; as discussed, Member States may deviate from the age of 16 set out in the GDPR, down to a lower limit of 13 years.

96 This conclusion is conditional and requires further investigation. It may also be argued that the European Commission could take into account the GDPR's requirements for parental consent, and the resulting risks of unlawful processing and the fundamental rights of the child, as part of the risk assessment and appropriate measures under Article 28 of the DSA. As the DSA Guidelines themselves make no reference to Article 8 of the GDPR, our tentative conclusion is that the European Commission does not consider this standard to be part of their assessment framework under Article 28 of the DSA.

97 In a comprehensive compliance analysis, the rights of the data subject (such as access, erasure and rectification), the role of the controller and processor, and international transfers would also merit further elaboration. These are not considered in this summary, but their application to age verification by the EDPB is discussed in the following sub-chapter.

The processing of personal data must have a valid legal basis.[98] Most relevant to age verification is compliance with a legal obligation; if legislation requires a platform to prevent use by minors, then this in principle provides a valid legal basis for the processing of personal data for this purpose.[99] However, the data processing must be *necessary* for compliance, and the purpose cannot therefore justify excessive processing. Furthermore, the legal obligation must serve a public interest objective and be proportionate to the aim pursued.[100] The legal obligation may specify certain aspects of the application of GDPR rules, for example with regard to 'the types of data which are subject to the processing; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing'.[101]

The GDPR therefore leaves some scope for national and EU legislators to impose obligations on private parties regarding the processing of personal data. However, this scope is limited by the requirements of necessity and proportionality.[102] Within these frameworks, the legal obligation can therefore also contribute to data protection by clarifying the conditions for processing, for example by specifying aspects such as the storage period or the necessary protective measures. The preconditions from Article 28(3) of the DSA discussed earlier are an example; this provision clarifies which data are (not) included in the processing obligation under Article 28(1) of the DSA. The Australian law, discussed in Chapter III, although not part of the GDPR framework, imposes different but comparable stipulations as to which data are (not) covered by the age assurance obligation.

In the context of *voluntary* age verification, a platform might, depending on the circumstances of the case, be able to rely on the user's consent; a task carried out in the public interest; and/or the legitimate interests of the controller or of third parties.[103] Since this report focuses on legal obligations, these scenarios are not considered in further detail.

In addition to the valid legal basis, the GDPR also sets out other legal principles of processing. Highly relevant in the context of age verification is purpose limitation. This principle entails that data collected for one purpose, subject to certain exceptions, should in principle not be used for other purposes.[104] This purpose limitation is also regularly reiterated in relevant regulations on age verification.[105] Purpose limitation is therefore an important principle to prevent age verification data from being misused by platforms, for example as input for AI training or microtargeting. Purpose limitation excludes such further processing in principle.[106]

A related principle is data minimisation. This means that no more data is processed than is necessary for the specific purposes.[107] In the case of age verification, this is a relevant principle, as the analysis revolves around a relatively simple, binary piece of data: is the user of legal age, or not? To verify this, additional information is often required, but there is also a risk of excessive, unnecessary processing. A simple example is that a date of birth contains more information than just whether the person is of legal age;

98 GDPR, Article 6 in conjunction with Article 5(1).
99 GDPR, Article 6(1).
100 GDPR, Article 6(3).
101 GDPR, Article 6(3): the GDPR cites as examples "the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing".
102 Ibid.
103 GDPR, Article 6(1). In the context of age verification, it is worth noting that Article 6(1)(f), the basis for legitimate interest, requires a balancing of interests, including fundamental rights and particularly in relation to children ("processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.").
104 GDPR, Article 5(b).
105 See Chapter III of this report.
106 For exceptions, see GDPR, Article 6(4).
107 GDPR, Article 5(c).

where possible, data minimisation requires that only the fact of being of legal age be processed, and not the full date of birth. Similarly, a passport contains considerably more information than just the date of birth alone (passport photograph, full name, nationality, place of birth, etc.). In the design of advanced verification technologies, data minimisation is a complex and significant consideration. A related principle is storage limitation: personal data should not be retained for longer than is necessary for the purposes of processing.[108]

Also relevant to age verification and child protection are the principles of accuracy (preventing inaccuracies, updating and rectifying where possible), and integrity and confidentiality (taking appropriate organisational measures to secure data and protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage).[109]

These principles are also further elaborated in specific GDPR provisions, which regulate, among other things, the transparency of processing, security measures and procedures for data breaches. In addition, the GDPR also grants specific rights to the end user, including the right to be informed about the processing; to access their data; and to have the data erased or corrected. [110] In accordance with the principle of privacy by design, age verification systems must also be designed in such a way that the controller can comply with these obligations.[111]

EDPB Statement 1/2025 on Age Assurance

In 2025, the European Data Protection Board (hereinafter 'EDPB') published a statement on age assurance, applying the principles of the GDPR to this practice. The EDPB's main recommendations are as follows:

> **A risk-based approach:** prior to implementing age verification, the platform must carefully determine whether this measure is necessary and proportionate in relation to the specific risks associated with its service. The interests of the child must be the primary consideration in this regard. The appropriate form for this assessment is a Data Protection Impact Assessment (DPIA), in which risks are identified and mitigation measures proposed.
>
> **Risk mitigation:** Age verification must not provide service providers with new ways to identify, locate, profile or track individuals. Effective alternatives must be offered to users who do not wish to use a particular verification method.
>
> **Data minimisation and purpose limitation**: Data processing must not go beyond what is necessary. For example: instead of age, legal age may be processed, and privacy-enhancing technologies such as third-party age assurance tokens may be used for this purpose (already discussed in the context of the DSA Guidelines).
>
> **Effectiveness:** Age verification must demonstrably achieve an adequate level of effectiveness. This requires periodic evaluation, based on (a) accessibility, (b) reliability, and (c) robustness. This evaluation requirement also applies where third-party services are used.
>
> **Lawfulness, fairness and transparency:** the processing must have a valid basis (such as, where applicable, a legal obligation). In the interests of transparency, certain information must be

108 GDPR, Article 5(e).
109 GDPR, Article 5.

shared with the data subject.[112] In particular for children, care must be taken to ensure that this information is shared in an understandable manner.

Automated decision-making: The use of automated decision-making in age verification may have legal consequences for the data subject, or otherwise significantly affect them, and must therefore be accompanied by appropriate measures to enable the data subject to exercise their rights (challenge the decision, request human intervention, express their views).[113]

Data protection by design and by default: Age assurance must take into account the most privacy-friendly methods and technologies ('state of the art'). Based on the current state of the art, the EDPB recommends considering device-based solutions, which can achieve unlinkability and selective disclosure.[114] In addition, batch issuance or single-use credentials and (as in the DSA guidelines) zero-knowledge proofs are recommended in contexts where there is a high risk to privacy.[115]

Security: The risk of a data breach can be mitigated through pseudonymisation and encryption. A no-log policy may stipulate that, once age has been verified, the personal data used for this purpose is no longer stored. Should a data breach nevertheless occur, the controller must be able to respond in a timely manner.

Accountability: The controller must be able to demonstrate compliance with the preceding principles. This requires adequate documentation and a clear division of responsibilities, so that age verification can also be audited by competent authorities.

The EDPB does not express a clear preference when it comes to choosing between different assurance methods. Mandatory verification is generally considered, from the perspective of the GDPR, to be the most intrusive measure, but this assumption does not hold true in all cases.[116] Depending on the implementation, age estimation can also be highly intrusive, and the risks associated with verification can also vary considerably.[117]

110 GDPR, Articles 13–17.
111 GDPR, Article 25.
112 Namely: what personal data is processed, and how; whether third parties are involved in the processing, and if so, who these third parties are and who the controller and processors are in this context; whether the data is shared with third parties or transferred to third countries; how long the personal data will be stored, or, if this is not possible, the criteria used to determine the storage period; and what rights the data subject has in relation to their personal data (e.g. Articles 15 to 22 of the GDPR), including how they can challenge an incorrect decision resulting from age verification. EDPB Statement, para. 24.
113 EDPB Statement, recitals 27–29. The recitals of the GDPR further state that automated decision-making which produces legal effects concerning the data subject or which otherwise significantly affects the data subject: "Such measure should not concern a child." However, the predecessor of the EDPB (the Article 29 Working Party) concludes that exceptions to this rule are possible under limited circumstances, for example where this is necessary to protect their welfare. See also: Article 29 Working Party (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.
114 By way of explanation, the EDPB states the following: "The unlikability property implies that it is impossible to associate or correlate different data items, actions or transactions to a specific data subject. Selective disclosure is a feature of tokens, credentials and attestations that allows data subjects to share only the information they want with specific parties on a case-by-case basis."
115 By way of explanation, the EDPB states the following: "Batch issuance relies on responding to one credential request from the data subject with a set or group of credentials produced at the same time. A zero-knowledge proof is a protocol in which one party (the prover) can demonstrate another party (the verifier) that some given statement is true, without conveying to the verifier any information beyond the mere fact of that statement's truth."
116 A similar point is also made in the Guidelines under Article 28 DSA – see para. 33: "The Commission notes that a lower accuracy of age estimation solutions does not automatically equate to a lower impact on the fundamental rights and freedoms of recipients, as less accurate solutions may process more personal data than more accurate ones."
117 See footnotes 24 and 26 above. Shaffique, M. & van der Hof, S., 2026. Behavioural profiling for age assurance: do the ends justify the means?, International Data Privacy Law, 16(1),https://doi.org/10.1093/idpl/ipaf012.

The proportionality of age verification

In the worst-case scenario, mandatory verification would amount to sharing identifying documents, such as a passport or credit card, directly with the platform. However, independent infrastructures can, in theory, offer a significantly higher level of protection: with EDPB best practices such as zero-knowledge proofs, in principle no identifying information is shared with the platform. The EU Age Verification App supports Member States in developing such a solution (see Chapter II.1.2).

Nevertheless, risks remain: these include the risk of data breaches and surveillance by (domestic or foreign) governments. Verification systems may also exclude certain groups, such as non-EU migrants without the necessary identity documents, as well as those with low digital literacy. To limit the risk of unjustified exclusion, it is recommended that a variety of verification options be offered (for example, a credit card in addition to an ID card). Another option, which has not yet been fully developed within existing frameworks, is the possibility of physical age verification (highlighted below).

The extent to which age verification restricts users' rights, and is proportionate to the interest served, therefore depends to a significant extent on details of its implementation. The effectiveness of the measure is also relevant to this proportionality assessment. It should be clear that even the strictest verification methods have vulnerabilities, particularly due to potential assistance from adults and/or the use of VPNs. In terms of proportionality, age verification also requires efforts from end-users and the government, which are taken into account in a proportionality assessment.

One hypothetical safeguard for vulnerable groups is integration with physical age verification. In theory, trusted parties, such as libraries, could be designated as distribution points for verification codes, based on a physical check, without the registration of any personal data. Individuals who are unable or unwilling to participate in digital verification could report to participating organisations to receive an anonymous verification token. For marginalised groups (such as those with low digital literacy and non-EU migrants without the necessary documentation), as well as for users with a particularly high interest in privacy (such as journalists), this could potentially be a valuable alternative to digital verification. However, this possibility has not yet been widely discussed in relevant policy circles and warrants further investigation.

The proportionality of age estimation

The privacy risks associated with age estimation differ from those of age verification, but are not necessarily lower. Whilst age verification, in principle, requires the platform to disclose very little information, age estimation relies on large-scale data collection and processing by the platform or by third parties. Chapter III discusses, in the Australian context, a comprehensive list of potential data sources that may be used for this purpose. The extent to which these practices are also permitted under EU law is open to question.

The DSA assumes that the platform is not obliged to store additional data about the user, apart from their age. Nevertheless, most commercial platforms are presumably capable of making estimates, as they already collect a great deal of user information for commercial purposes. However, these practices vary by platform and over time, and may create a perverse incentive for (smaller and non-commercial) platforms that are indeed restrained in their user profiling. Furthermore, there are complex interactions with the GDPR legal basis for processing children's data: as discussed in Chapter II.3.1, extensive profiling of minors for commercial purposes is often prohibited, precisely because there is no valid legal basis for it.[118]

118 Where the age of a minor is known, the provider can no longer rely on consent unless parental consent has also been obtained. The provider may still invoke the performance of the service contract as a legal basis, but this basis only supports processing that is objectively necessary to provide the service and, in principle, does not justify data collection for commercial profiling

In summary, the possibilities for lawful age estimation in the EU are limited by the GDPR and the Charter, and are presumably also more limited than in Australia. A comprehensive analysis goes beyond the scope of this report, but as a tentative conclusion, it appears that a legislative amendment would likely be required to enable a comparable level of profiling (for example, a legal basis for processing at national level, or an amendment to the restrictions in Article 28(3) of the DSA). Even then, the necessity and proportionality of this legislative amendment would still be required in order to comply with the GDPR.

Also relevant to this proportionality analysis is the fact that age estimation entails risks of discrimination and unjustified exclusion. Profiling techniques are generally less reliable when applied to minority groups, who differ from the majority population for which the techniques were developed. A concrete example is the reduced effectiveness of facial recognition software for non-white ethnicities. These risks can be mitigated through audits, appeal procedures and other safeguards, but cannot be ruled out completely.

The limited effectiveness of age estimation is also a factor in its proportionality. As with verification, adults or VPNs can help minors to circumvent the checks. Even without deliberate circumvention, profiling is relatively unreliable, and even less so when creating new accounts, as there is then no behavioural history available for profiling. Chapter III.1.4 discusses the effectiveness of age estimation in further detail, drawing on concrete experiences in Australia.

Discussion

In summary, the GDPR provides important framework conditions for age verification, including general principles and several EDPB-specific recommendations. Central to this, as with the DSA guidelines, is a risk-based approach, in which the importance of age verification is weighed against the potential privacy risks. The interests of the child are a first consideration here. The greater the risks a service poses to the rights of the child and to other interests, the more this justifies stringent forms of age verification. The fundamental rights considerations at play – both for and against age verification – are explained in more detail in the following chapter.

Future legislation could prescribe a specific assurance method. However, the GDPR does require that, as a processing ground, this legal requirement meets the conditions of necessity and proportionality. Once again, a risk-based balancing of interests is central here. The legislator must be able to justify why the relevant verification obligations serve a legitimate purpose, are necessary to achieve this purpose, and are proportionate to the risks to the fundamental rights of data subjects. The EDPB also highlights other safeguards, such as data minimisation, accountability obligations, and freedom of choice for the data subject. Even taking these safeguards into account, this proportionality assessment appears challenging; both verification and estimation entail significant drawbacks, which put privacy under pressure, may exclude or disadvantage vulnerable groups, and, despite these costs, are still limited in their effectiveness. Data protection law therefore requires caution and restraint for the introduction of any age assurance obligations – a conclusion that is also supported by the constitutional analysis in Chapter II.5 below.

purposes. However, in order to estimate the user's age, such profiling data would need to be collected. One possible interpretation is that this profiling is only permitted until it is established that the user is a minor, after which the data must be deleted immediately.

2.4 Digital Fairness Act (proposal)

A new legislative proposal is currently being drafted at EU level: the Digital Fairness Act (DFA). This report only touches on the subject briefly, as the DFA is still at an early stage. A draft bill has not yet been published, so little is known about its exact content.

The DFA was prompted by a 2024 review that identified several shortcomings in online consumer protection. The intention is to address abuses such as the following: (1) unfair commercial practices involving the use of dark patterns; (2) misleading marketing by influencers; (3) addictive design of digital products; and (4) unfair personalisation practices.[119] A public consultation was held in the summer of 2025, and the first draft legislation is expected in the autumn of 2026.[120] Proposals for a minimum age for social media are also regularly linked to the DFA.[121]

As an initiative under consumer law, the DFA falls under the Directorate-General for Justice and Consumers (DG JUST). This is in contrast to the DSA and AVMD, which fall under the Directorate-General for Communications Networks, Content and Technology (DG CONNECT). For the DSA, as discussed, DG CONNECT is also the supervisory authority.

2.5 Fundamental rights and the rights of the child

n addition to sector-specific legislation and regulations, fundamental rights also apply to minors in the digital context. These fundamental rights have also significantly influenced the applicable legislation. Key instruments in this area are the European Convention on Human Rights ('the ECHR'), the Charter of Fundamental Rights of the European Union ('the Charter'), and the International Convention on the Rights of the Child ('the CRC').[122] These fundamental rights set limits on the policy scope of public authorities, and in certain cases also of platform companies and other private parties.[123] Fundamental rights also shape the interpretation of legislation and regulations, and provide an assessment framework for principles such as necessity and proportionality. Below, general principles are discussed first, followed by their application to social media by authoritative bodies.

2.5.1 Freedom of expression and information

Freedom of expression is recognised as a fundamental right for both adults and children. In most definitions, this right is also subsumed under a broader right to freedom of information, which protects not only the speaker but, in a broader sense, 'the freedom to receive or impart information or ideas'.[124] The Convention on the Rights of the Child adds that freedom of information applies to children 'either orally, in writing or in print, in the form of art, or through any other media of the child's choice'.[125]

Freedom of information is not unlimited. The grounds for restriction are formulated differently across treaties, but must in any case be provided for by law and must be necessary and proportionate in relation to specific objectives in the public interest, such as the protection of public health and public morals.[126]

---

119 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14622-Digital-Fairness-Act_en.
120 Ibid.
121 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202601708.https://www.euractiv.com/news/capitals-quizzed-on-how-child-safety-should-fit-into-digital-fairness-rules/.
122 Article 24 of the Charter of Fundamental Rights of the European Union is also relevant. See also: European Commission (2021), Communication on the EU Strategy on the Rights of the Child, COM(2021) 142 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0142.
123 See, inter alia, Fornasier, M. (2015). The impact of EU fundamental rights on private relationships: direct or indirect effect?. European Review of Private Law, 23(1).
124 ECHR, Article 10(1).
125 CRC, Article 13(1).
126 CRC, Article 13(1).

The Convention on the Rights of the Child also contains a supplementary provision on access to information: Article 17 requires recognition of "the important function performed by the mass media" and obliges States to "ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health". Specific recommendations are linked to this principle, primarily aimed at stimulating the production of high-quality and diverse media content for children. States also undertake to "encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of Articles 13 [freedom of expression] and 18 [parental responsibilities]".[127]

A minimum age for social media jeopardises young people's freedom of expression and information. In principle, there is no direct impact on adults, as they retain the right to use social media without restriction. However, age verification systems may *indirectly* restrict adults' rights, insofar as they limit users' privacy. Age verification can also safeguard anonymity, but depending on the implementation context, there may be risks of (unintended) de-anonymisation and other privacy risks, for example through data breaches. These concerns may have a chilling effect on users, meaning they may be less willing to make (full) use of their freedoms of information. The perception of anonymity and privacy risks also plays a role here. In addition to a chilling effect, there is also a risk of unjustified exclusion of adults from vulnerable groups (e.g. migrants, users lacking digital literacy), whose freedom of expression is thereby also restricted.

2.5.2 Privacy and data protection

The right to privacy is protected by Article 8 of the ECHR. In the EU Charter, alongside privacy (Article 7), the right to data protection (Article 8) is also protected as an independent fundamental right, which specifically focuses on the processing of information (as opposed to, for example, physical forms of privacy related to bodily integrity or the living environment). The Convention on the Rights of the Child also protects the privacy of the child (Article 16).

As discussed in Chapter II.3, age verification constitutes a restriction on the right to privacy and the right to data protection. The GDPR serves here as an elaboration of the fundamental right to data protection, invoking concrete and enforceable rules to give substance to the general fundamental right. In this sense, the analysis in Chapter II.3 remains the guiding principle in the assessment of privacy and data protection aspects relating to age verification. These rules from the GDPR must be applied in the light of the underlying fundamental rights. These fundamental rights may also have an additional constitutional effect by rendering incompatible legislation inoperative.

The previous sub-chapter (II.5.1) also showed that data protection has indirect implications for the exercise of other fundamental rights, such as freedom of expression and information. It follows from this GDPR analysis that proportionality can be safeguarded in part by measures such as privacy-protecting infrastructure, freedom of choice for the user, redress mechanisms for unjustified exclusion, and, where appropriate, options for anonymous physical verification, etc. Proportionality is also linked to the scope of the minimum age; for example, whether it applies to all social media, or only to certain unsafe services. These considerations regarding proportionality are also addressed in Chapter 4 under the policy considerations.

127 CRC, Art 17(e).

2.5.3 Other fundamental rights and child safety

Whilst freedom of information and the right to privacy apply to all persons, the Convention on the Rights of the Child also mentions other relevant rights specific to children.

The central principle for the protection of children, set out in Article 3 of the Convention on the Rights of the Child, states: "In all actions concerning children […] the best interests of the child shall be a primary consideration."[128] Naturally, the concrete application of this principle remains controversial: the point of contention is precisely whether children benefit from measures such as a minimum age. Access to social media has both advantages and disadvantages for the interests of the child, which may also vary from one individual to another. In practical terms, the function of Article 3 is to place a holistic assessment of all the relevant advantages and disadvantages for children at the centre of the fundamental rights analysis. In the following sub-chapter, Article 3 is also linked to the precautionary principle, which urges governments to act even in circumstances of (scientific) uncertainty.

Article 31 of the Convention on the Rights of the Child protects "the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural and artistic life". States Parties shall promote this right and encourage appropriate and equal opportunities for all in this regard. Social media is a popular environment for cultural and artistic exchange, so a minimum age may limit young people's participation in this sphere. One possible safeguard, which has also been recommended by other authors, is to combine the regulation of social media with proactive incentives for other forms of leisure activity.[129]

Article 33 of the Convention on the Rights of the Child requires "all appropriate measures […] to protect children from the illicit use of narcotic drugs and psychotropic substances as defined in the relevant international treaties". Social media can act as a distribution channel for such substances. It is worth noting, however, that tobacco and nicotine-containing products such as vapes do not, in principle, fall under this provision. According to the Committee on the Rights of the Child, however, tobacco products do fall within the scope of Article 24 of the Convention on the Rights of the Child, concerning the right to health. States Parties therefore have a responsibility to take appropriate measures to protect children from both drugs and tobacco products, including when these are distributed via social media.[130]

Article 34 of the Convention on the Rights of the Child obliges States Parties "to protect the child from all forms of sexual exploitation and sexual abuse". Once again, social media is a clear risk factor. In one study, 13% of Instagram users aged between 13 and 15 reported that they had received unwanted sexual advances on the platform in the past seven days.[131] Internal research at Snapchat and TikTok points to similar patterns.[132] A further discussion of the scientific evidence on the effects of social media follows in the next sub-chapter.

These provisions do not, *in themselves*, appear to justify a statutory minimum age. Drug sales and sexual exploitation are very serious abuses, but for most platforms they account for only a small minority of all activity. Should a ban be based solely on these grounds, and apply to all social media, then its

128 https://wetten.overheid.nl/BWBV0002508/2002-11-18 (The Dutch translation of the Convention on the Rights of the Child states 'the first consideration', but in the original English it is merely 'a first consideration'. The authentic English version is thus, in a subtle way, less categorical.

129 Bursztyn, L. et al. (2026). Why Bans Fail: Tipping Points and Australia's Social Media Ban. University of Chicago Becker Friedman Institute for Economics Working Paper 2026-57.https://bfi.uchicago.edu/wp-content/uploads/2026/04/BFI_WP_2026-57.pdf.

130 Among the major platforms, Snap, among others, has been linked to the illegal sale of vapes to minors. See Chapter II.1.5.

131 Béjar, A. (2024, 6 May). How to reduce the sexual solicitation of teens on Instagram. After Babel.https://www.afterbabel.com/p/make-social-media-safe-for-teens,

132 Haidt, J., & Rausch, Z. (2025a, 9 January). TikTok is harming children on an industrial scale. After Babel.https://www.afterbabel.com/p/industrial-scale-harm-tiktok. Haidt, J., & Rausch, Z. (2025b, 16 April). Snapchat is harming children on an industrial scale. After Babel.https://www.afterbabel.com/p/industrial-scale-snapchat.

proportionality could potentially be called into question. Targeted measures against the illegal activity in question might then strike a better balance between the conflicting fundamental rights. It should be noted, however, that platforms have been subject to supervision for many years to combat harm to underage users, but have so far delivered limited results in this area. The alternative of targeted solutions for specific problems therefore does not appear to be (fully) effective either.

A minimum age appears to be better justified by a *combination* of various policy grounds, with an emphasis on general effects on young people's well-being and mental health, and with specific fundamental rights risks relating to drugs and sexual exploitation as additional considerations. This brings Article 3 of the Convention back into focus: the duty to give primary consideration to the best interests of the child.

2.5.4 The precautionary principle and the scientific basis for a minimum age

The precautionary principle implies that the fundamental rights protection of children can justify intervention even in the absence of definitive evidence regarding potential harm.[133] In other words, 'better safe than sorry' serves as the guiding principle.[134] The precautionary principle originated in environmental law and has since become commonplace in the assessment of scientific evidence in international and constitutional matters. The UNESCO World Commission on the Ethics of Scientific Knowledge has developed the following working definition:

> When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, actions shall be taken to avoid or diminish that harm.
>
> Morally unacceptable harm refers to harm to humans or the environment that is
>
> - threatening to human life or health, or
> - serious and effectively irreversible, or
> - inequitable to present or future generations, or
> - imposed without adequate consideration of the human rights of those affected.[135]

Several academics argue that the precautionary principle also applies to child protection outside the environmental context and in the digital environment.[136] The precautionary principle is also common in regulatory practice. A key example of this is the general ban on access to pornography: here too, there is a lack of conclusive scientific evidence regarding the harmful effects on children.[137] Nevertheless, this policy is widely accepted and even considered necessary for the protection of children's rights. The precautionary principle is not codified as such in the Convention on the Rights of the Child, but is generally associated

133 Lievens, E., 2021. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. Nordic Journal of Human Rights, 39(2), pp.128–145.

134 Livingstone, S. et al., 2024. Children's rights and online age assurance systems: The way forward. The International Journal of Children's Rights, 32(3), pp.721-747.

135 UNESCO World Commission on the Ethics of Scientific Knowledge and Technology (2005). 'The Precautionary Principle'.https://unesdoc.unesco.org/ark:/48223/pf0000139578.

136 Martuzzi, M. & Tickner, J. (2004). The precautionary principle: protecting public health, the environment and the future of our children. World Health Organization. Lievens, E., 2021. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. Nordic Journal of Human Rights, 39(2), pp.128–145.

137 Nair, A., 2018. The regulation of Internet pornography: Issues and challenges. Routledge. See also: Lievens, E., 2021. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. Nordic Journal of Human Rights, 39(2), pp.128-145.

with Article 3(1) and the duty to treat the best interests of the child as a primary consideration.[138]

For social media, the precautionary principle is highly relevant because the effects on children's well-being are not (yet) fully established. A brief overview of the current state of scientific knowledge is provided below. Given the complexity of this subject matter, and the limited scope of this report, this cannot be an exhaustive account. Caution is indeed required here: some authors note that leading scientific syntheses also reach divergent conclusions, despite the fact that they draw on comparable evidence.[139] Clearly, there is considerable leeway for nuance and interpretative choice when assessing the available research. This, too, contributes to the relevance of the precautionary principle and the need to be prepared to take political action even in circumstances of scientific uncertainty.

When it comes to mental and physical health, social media use shows clear negative correlations. However, the phenomenon varies by population group (including geographically and by gender), and there are also doubts regarding causality. A recent review of the influential but controversial World Happiness Report 2026 (WHR 2026) highlights the following findings, amongst others:

- Life satisfaction decreases as social media use increases, for 15-year-olds in countries included in the PISA study (including the Netherlands).[140]
- The correlation is stronger for girls (~1 point on a scale of 10) than for boys (~0.5 points), and stronger in affluent Western countries.

Disagreement persists among scientists regarding the interpretation of the available data. According to Jonathan Haidt, a prominent advocate of minimum age limits, there is sufficient evidence to establish negative causal effects of social media. Critics, on the other hand, point to the limited effect size of many studies; the limited replication and available counter-evidence; and the lack of strong causal evidence. The most significant declines appear to be concentrated in a relatively small group of very intensive users, and the question remains whether their excessive use is the cause of their mental and social problems or merely a consequence. It is also the case that moderate use (<1 hour per day) scores better than non-use.[141] Natural experiments raise similar questions: for example, in developing countries, where social media has only recently been adopted by young people, well-being has not measurably declined.[142]

Given this ongoing scientific disagreement, the precautionary principle remains highly relevant. Definitive empirical evidence on the precise effects of social media is not available and may never be. Social media

138 Lievens, E., 2021. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. Nordic Journal of Human Rights, 39(2), pp.128-145. Livingstone, S., Nair, A., Stoilova, M., van der Hof, S. and Caglar, C., 2024. Children's rights and online age assurance systems: The way forward. The International Journal of Children's Rights, 32(3), pp.721-747. See also: UN Committee on the Rights of the Child (2013), General comment no. 14 on the right of the child to have his or her best interests taken as a primary consideration. CRC/C/GC/14. Eekelaar J. & Tobin J., 2019. 'Article 3 the Best Interests of the Child' in: Tobin, J. (ed), The UN Convention on the Rights of the Child: A Commentary (Oxford: Oxford University Press 2019).

139 Helliwell, J. F. et al. (eds.), 2026. World Happiness Report 2026. University of Oxford: Wellbeing Research Centre. See also: National Academies of Sciences, Engineering, and Medicine, 2024. Social Media and Adolescent Health. (The National Academies Press). https://www.nationalacademies.org/projects/HMD-BPH-21-14/publication/27396, Office of the Surgeon General, 2023. Social Media and Youth Mental Health: The US Surgeon General's Advisory. US Department of Health and Human Services. https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf. American Psychological Association, 2023. Health Advisory on Social Media Use in Adolescence (APA Press). https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use. A relevant synthesis in the Dutch context is the Guideline on Healthy Screen Use 2025. Koning, I. et al., 2025. Guideline on Healthy Screen Use. Ministry of Health, Welfare and Sport. https://www.rijksoverheid.nl/documenten/rapporten/2025/06/17/richtlijn-gezond-schermgebruik-2025. At EU level, the Joint Research Centre and the European Centre for Algorithmic Transparency have produced a joint literature review, see: Beullens, K. et al., 2025. Minors' health and social media: an interdisciplinary scientific perspective, Publications Office of the European Union, JRC141090. https://data.europa.eu/doi/10.2760/3795891.

140 "Life satisfaction is highest at low rates of social media use and lower at higher rates of use, according to data from the Programme for International Student Assessment (PISA) covering seven internet activities for 15-year-old students in 47 countries (but not the NANZ countries, unfortunately)." Helliwell, J. F. et al. (eds.), 2026. World Happiness Report 2026. University of Oxford: Wellbeing Research Centre.

141 Ibid.

142 Ibid.

is considerably more complex in terms of its effects on well-being than, for example, tobacco products, as it is to a greater extent a social and cultural phenomenon, for which individual use also has indirect effects on societal developments and vice versa. Scientific studies can only examine the effects of individual choices – such as hours of use per individual – against the backdrop of a society where social media remains unavoidably prevalent and affects everyone to a greater or lesser extent, directly or indirectly. Consequently, the indirect ('second-order') effects of a collective ban therefore remain inherently uncertain. At the same time, there is sufficient evidence to substantiate a strong presumption and to justify policy-making beyond a reasonable doubt.

Furthermore, other policy grounds can be cited, in addition to (mental) health, for which more direct evidence exists. Firstly, social media is also linked to various forms of exploitation and abuse ('online harms'), for which the causal link with social media may be stronger. Although platforms also have obligations to prevent such abuse, complete prevention is not realistic given the current state of moderation technology, and monitoring these practices remains challenging in any case. In this context, a minimum age may be seen as a necessary alternative for tackling illegal content and practices that cause harm to minors. Secondly, many young people also indicate that they are dissatisfied with their own use of social media. Among students in the US, a majority would even prefer social media not to exist; they continue to use these services because others do, but would prefer that nobody used them.[143] The risks of exploitation and online harm, as well as the wishes of young people themselves, may provide additional grounds for a minimum age.

143 Bursztyn, L., Handel, B., Jiménez-Durán, R., & Roth, C. (2023). When Product Markets Become Collective Traps: The Case of Social Media. SSRN Electronic Journal.https://doi.org/10.2139/ssrn.4597079.

2.5.5 Positions taken by human rights organisations on minimum ages

Committee on the Rights of the Child: General Comment No. 25 on children's rights in relation to the digital environment

An authoritative interpretation of the Convention on the Rights of the Child has been developed by the UN Committee on the Rights of the Child in its General Comment No. 25 on children's rights in relation to the digital environment, published in 2021. In this document, the Committee emphasises the importance of the digital environment for children's access to information and freedom of expression.[144] It is worth noting, however, that this 'digital environment' is not synonymous with (commercial) social media. Indeed, the Committee emphasises that the government has a role in promoting the production and distribution of high-quality and 'age-appropriate' material. The Committee is clear in its recommendation that governments should not deliberately prevent access to electricity, mobile networks and the internet. However, when it comes to social media, it is not quite so categorical; a minimum age might however be in tension with the recommendation that "[c]ontent controls, school filtering systems and other safety-oriented technologies should not be used to restrict children's access to information in the digital environment; they should be used only to prevent the flow of harmful material to children."[145]

Is a minimum age for social media compatible with this principle? On the one hand, there may be tensions, because a minimum age prevents access not only to harmful material, but to all material on the regulated services, including harmless material. On the other hand, it can be argued that a minimum age, as such, is not 'safety-oriented technology', depending on the associated age verification rules, and could therefore fall outside the scope of this recommendation. Furthermore, the intention is to focus the minimum age on 'insufficiently safe' services, which contributes to its proportionality.[146]

Governments should also introduce legislation to protect minors from violence and (sexual) exploitation, including non-consensual sexual images; digital shaming and blackmail; and incitement to self-harm, suicide and eating disorders.[147] To this end, "preventive, safeguarding and restorative measures" are required, as well as "legislative and administrative measures to protect children from violence in the digital environment".[148] Children must also be protected from harmful goods and services, such as drugs and gambling. To this end, according to the UN, "robust age verification systems" are needed "to prevent children from acquiring access to products and services that are illegal for them to own or use."[149]

In summary, the General Comment paints a mixed picture of minimum age limits for social media. Although children enjoy freedom of expression and the right of access to information, the emphasis is primarily on access to media and the internet, but not to social media as such. The General Comment favours targeted measures against harmful content, as opposed to general access restrictions. At the same

144 UN Committee on the Rights of the Child. General comment No. 25 (2021) on children's rights in relation to the digital environment.https://digitallibrary.un.org/record/3906061?ln=en&v=pdf (hereinafter: 'General Comment No. 25'), para. 50 et seq. ("The digital environment provides a unique opportunity for children to realise the right to access to information. In that regard, information and communications media, including digital and online content, perform an important function. States parties should ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided for by law and is necessary for the purposes set out in Article 13 of the Convention.") Para. 58 et seq. ("The digital environment offers significant scope for children to express their ideas, opinions and political views. For children in disadvantaged or vulnerable situations, technology-facilitated interaction with others who share their experiences can help them to express themselves.")

145 General Comment No. 25, Para 56. The Committee also notes that "age-based or content-based systems designed to protect children from age-inappropriate content should be consistent with the principle of data minimization" (see also paragraph II.5.2 of this report).

146 Chapter IV provides further clarification on the categorical and risk-based interpretations of this principle. The tensions are most pronounced in a categorical approach, where all social media fall under the same minimum age. In a risk-based approach, the tension is reduced by focusing the age requirement on specific unsafe services. However, even on unsafe services, harmless content may exist alongside harmful content. In that sense, a tension remains between the General Comment and the proposal for a minimum age.

147 General Comment No. 25, paras. 80 and 81.

148 General Comment No. 25, paras. 81 and 82.

149 General Comment No. 25, para. 114 ("Such systems should be consistent with data protection and safeguarding requirements.")

time, there is a clear mandate for governments to intervene where children's safety is at risk, including through the use of age verification systems. Furthermore, the right of access to media is primarily fulfilled through positive obligations to promote high-quality media content.

Since the publication of the *General Comment* in 2021, the available evidence on the potentially harmful and addictive effects of social media has increased (see discussion in Chapter II.5.4). It can thus be argued that far-reaching protective measures, which in the General Comment are most explicitly directed at gambling and drug trafficking, may also be permissible for certain social media. In any case, it is clear that restraint and caution are advisable to avoid an infringement of freedom of expression, access to information, and privacy.

Other UN standards and positions

In their 2023 annual report, the Special Representative of the Secretary-General on Violence against Children spoke positively about age verification as a protective measure against online violence against minors.

> Several jurisdictions have introduced or are considering age verification or age assurance to limit children's access to age-inappropriate content that may be harmful but not illegal, such as sexually explicit or violent content. This is a crucial dimension of an effective response focused on prevention.[150]

However, the question of whether age verification is also an appropriate measure for social media remains open.

UNICEF has been critical of the Australian policy on a minimum age for social media. In an online press release dated 9 December 2025, UNICEF warned that "[a]ge restrictions alone won't keep children safe online".[151] Their main criticism is that social media can be enriching for young people ("for many children, especially those who are isolated or marginalised, it is a lifeline providing access to learning, connection, play, and self-expression"). In addition, UNICEF points to the possibility that a ban could be circumvented, either through "workarounds" or by switching to unregulated services.[152] Despite this criticism, the minimum age is not explicitly discouraged or declared incompatible with children's rights. However, minimum ages alone are not sufficient, according to UNICEF, and should form part of a broader package of child protection measures. The key recommendation is therefore that the minimum age should not replace, or divert resources from, investments in child protection measures by platforms.[153] UNICEF Australia has responded in a similar manner.[154]

Volker Türk, the UN High Commissioner for Human Rights, was relatively less critical of Australian policy during a press conference; he acknowledged that the desire to take stricter measures to protect children in the digital environment is understandable, and simply recommended that it is important to continue monitoring which policies are effective and to put the interests of the child first[155] .

150 United Nations, Human Rights Council. (2023). Annual report of the Special Representative of the Secretary-General on Violence against Children (A/HRC/52/61).https://docs.un.org/en/A/HRC/52/61, para. 74.
151 https://www.unicef.org/press-releases/age-restrictions-alone-wont-keep-children-safe-online.
152 Ibid.
153 Ibid. ("Age restrictions must be part of a broader approach that protects children from harm, respects their rights to privacy and participation, and avoids pushing them into unregulated, less safe spaces. Regulation should not be a substitute for platforms investing in child safety. Laws introducing age restrictions are not an alternative to companies improving platform design and content moderation.")
154 https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer.
155 "It's very important to keep monitoring what works, what doesn't work. The best interests of the child have to be taken into account."https://webtv.un.org/en/asset/k1n/k1npknnnv3.

Council of Europe: Commissioner for Human Rights

On 23 February 2026, Michael O'Flaherty, Commissioner for Human Rights at the Council of Europe, published a response to proposals from several member states to introduce a minimum age for social media. The thrust is similar to that of UN bodies such as UNICEF: minimum ages are not explicitly rejected, but caution and restraint are called for.[156] The main concern is that minimum ages must not serve as an alternative to, or distract attention from, the responsibility of platforms to create a safe environment for minors. As an example of such a policy, O'Flaherty praises the European Commission's recent enforcement actions against TikTok regarding its addictive design.[157]

Council of Europe, Parliamentary Assembly: Report on the Protection of Children against Online Violence (2024)

The Parliamentary Assembly of the Council of Europe, on the other hand, supports age restrictions. A report dated 27 March 2024 on The Protection of Children Against Online Violence recommends developing a "comprehensive legal framework", including "effective age verification obligations on websites providing goods and content which are not intended for children, and which would incur similar obligations in the offline world".[158] Three requirements are set for these verification techniques: "sufficiently reliable verification, complete coverage of the population and respect for the protection of the individual's data, privacy and security, especially confidentiality of information and minimising data exchange".[159] Once again, it is not made explicit whether social media should also fall under such an obligation, and the emphasis in this case is on pornography websites.

Council of Europe, Committee of Ministers: Recommendation CM/Rec(2026)4 on online safety and the empowerment of users and creators (2026).

The Committee of Ministers has issued a series of recommendations on internet freedoms and the protection of children in the digital environment.[160] The most recent and relevant is Recommendation CM/Rec(2026)4, which explicitly addresses recent discussions on age verification.[161] The key recommendation reads as follows:

> 75. In addition to other appropriate risk mitigation measures that may be adopted by platforms and in line with Recommendation CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, States should require the use of effective systems of age assurance to ensure children are protected from products, services and content in the digital environment which are legally restricted with reference to specific ages. In particular, such systems should be required for platforms that predominantly provide services or content that is legally restricted to protect children. Such systems should uphold human rights and use methods that respect freedom of expression and the protection of personal data and privacy and that are consistent with the best interests of the child. When requiring the implementation

156 "As several European countries consider introducing a minimum age for accessing social media platforms, I urge caution in imposing sweeping bans. The focus on restricting access should not divert attention from ensuring that platforms respect human rights through clear legal obligations, independent oversight, and effective accountability". https://www.coe.int/en/web/commissioner/-/regulate-platforms-not-children-council-of-europe-commissioner-for-human-rights-urges-caution-over-social-media-bans

157 https://www.coe.int/en/web/commissioner/-/regulate-platforms-not-children-council-of-europe-commissioner-for-human-rights-urges-caution-over-social-media-bans

158 Council of Europe, Parliamentary Assembly, 2024. Report on the protection of children against online violence. Document 15954.https://pace.coe.int/en/files/33405/html.

159 Ibid., para. 24.

160 See, inter alia: Council of Europe, Committee of Ministers, 2018. Recommendation CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

161 Ibid. Also indirectly relevant are paragraphs 76 and 77, concerning the protection of children in a broader sense and the facilitation of content labelling by platforms.

> of such systems, States should provide safeguards to ensure they do not result in disproportionally excluding children from online spaces and restricting their right to participate in debates on matters of public interest. Safeguards should also be provided to ensure that these systems do not create or exacerbate exclusion from the online space of people in situations of vulnerability and at risk of discrimination.[162]

This approach is therefore comparable to the DSA Guidelines: the strongest recommendations are aimed at platforms offering age-restricted content, such as pornography and gambling platforms. A categorical age verification obligation for social media is not (explicitly) deemed necessary, but is not ruled out either. Member States appear to be free to designate social media as such as an age-restricted service ("services […] in the digital environment which are legally restricted with reference to specific ages") for which age verification is necessary. At the same time, this recommendation does warn against the disproportionate exclusion of minors. Whether a minimum age for social media would be disproportionate is not explicitly addressed and may require an analysis based on the specific circumstances of the case. It also warns against the exclusion of vulnerable groups in the implementation of age verification (see also Chapter II.5.1 above).

2.5.6 Discussion

The constitutional framework makes clear that, when regulating social media with a view to protecting minors, all relevant interests must be carefully weighed up. In doing so, the interests of the child must be taken as a first consideration. Governments have a duty to organise a healthy and diverse media landscape for children, in which freedom of choice is a key value but protection against content that is detrimental to the child's development must also be addressed. In a context of scientific uncertainty regarding the precise (positive and negative) effects of social media and of a potential ban, the precautionary principle also plays a role in justifying government intervention.

However, there is still disagreement regarding the concrete application of these principles. Many international bodies emphasise the risks that minimum age limits pose to freedom of information and privacy, but do not go so far as to completely advise against them. They limit themselves to warning that a nuanced and careful approach is required, with a sound, proportionate policy design and attentive monitoring during and after implementation.

Age assurance, in particular, remains a key concern; strict age verification requirements have a significant impact on user privacy—including that of adult users, not just minors—and should be applied with caution. In the context of social media, these privacy risks are significant due to the important role these services play in social interaction and public debate. Unjustified exclusion or disproportionate surveillance (of adult users) resulting from flawed or excessive age verification threatens not only privacy but also freedom of information and freedom of expression, with a potential chilling effect.

Whether strict verification requirements are indeed justifiable remains, in part, an empirical assessment based on the proven effectiveness of these measures (see Chapter III.1 on this subject). However, reaching a definitive conclusion is challenging, as these are relatively new and experimental techniques, for which there are few precedents regarding large-scale implementation on social media.[163] Based on the Australian example, discussed in Chapter III.1, there is reasonable doubt regarding the effectiveness of age estimation. In any case, it is relevant to the proportionality assessment that both verification and estimates remain vulnerable to circumvention through adult assistance and the use of VPNs.

---

162 Ibid, para. 75.

163 Researchers José van Dijck and Bart Jacobs, for example, advocate a decentralised approach to digital identity, which differs significantly from current European policy. Van Dijck, J. & Jacobs, B., 2024. Electronic identity services as sociotechnical and political-economic constructs. New Media & Society 22(5). https://doi.org/10.1177/1461444819872537.

In any case, the principles of the GDPR from the previous chapter must also be observed, so that age verification is not organised in a more intrusive manner than necessary. A constitutional analysis therefore supports not only the choice between age estimation or verification, but also the further design and implementation of the chosen method.

The following chapter will show that other parties (end-users, government bodies) do indeed take the view that strict minimum age limits are incompatible with fundamental rights. If European governments codify such a policy, critical constitutional scrutiny is to be expected.

3 Comparative legal analysis

This chapter examines recent legislation that has sought to introduce a minimum age for social media. This is not an exhaustive overview but a selection of two leading cases: Australia and France.[164] Australia is the first country to introduce a statutory minimum age for social media, and therefore offers empirical insights into enforceability and other consequences. The French law is still in preparation, but illustrates the challenges at play in the European context and the interactions between national legislation and EU law.

3.1 Australia

On 29 November 2024, Australia became the first country to introduce a statutory minimum age for social media. This was achieved through an amendment to the Online Safety Act. Following a preparatory period of approximately one year, the legislation finally came into force on 10 December 2025.

3.1.1 Scope of application: To which services does the minimum age apply?

The Australian minimum age of 16 applies to "age-restricted social media platforms", defined as electronic services that meet the following conditions:

i. the sole purpose, or a significant purpose, of the service is to facilitate social interaction between 2 or more end-users;
ii. the service allows end-users to link with, or interact with, some or all of the other end-users;
iii. the service allows end-users to post material on the service;
iv. such other conditions (if any) as are set out in the legislative rules[165]

Outside this definition, electronic services may also be designated directly through legislative rules. The Minister for Communications is authorised to do so only if he considers it reasonably necessary to minimise harm to underage users.[166] Procedural conditions also apply to this measure.[167]

However, exceptions apply to certain categories of services: if none of the material on the service is accessible to, or distributed to, one or more end-users in Australia; or if the service is exempted by legislative rules.

164 For an overview of similar legislative proposals, see: Jahangir, R. & Hendrix, J., 2026. Tracking Efforts To Restrict Or Ban Teens from Social Media Across the Globe. Tech Policy Press.https://www.techpolicy.press/tracking-efforts-to-restrict-or-ban-teens-from-social-media-across-the-globe/. For a detailed discussion of the German context, as a further example, see: Galissaire, J., 2025. Mind the Gap: Age Assurance and the Limits of Enforcement under EU Law. Interface.https://www.interface-eu.org/publications/age-assurance-gap.

165 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Section 63C(1)(a). The supplementary 'notes' provide the following further clarification: "(2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes. Social purposes does not include (for example) business purposes. (3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes: (a) the provision of advertising material on the service; (b) the generation of revenue from the provision of advertising material on the service."

166 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Section 63C(1).

167 Ibid. ("(5) Before making legislative rules specifying an electronic service for the purposes of paragraph (1)(b): (a) the Minister must seek advice from the Commissioner, and must have regard to that advice; and (b) the Minister may seek advice from any other authorities or agencies of the Commonwealth that the Minister considers relevant, and may have regard to any such advice.")

The Minister for Communications, Anika Wells, issued such rules on 29 July 2025. A few further amendments were made on 25 March 2026.[168] These rules contain important exceptions for certain parties; services with the following sole or primary purpose are therefore exempt from the minimum age requirement:

- Communicating by means of messaging, email, voice calling or video calling;
- Playing online games with other end-users;
- Sharing information (such as reviews, technical support or advice) about products or services;
- Participating in professional networking and professional development;
- Supporting the education of end-users;
- Supporting the health of end-users;
- Facilitating communication between educational institutions and students or students' families;
- Facilitating communication between healthcare providers and the recipients of their services;[169]

Specifically, the scheme applies to the following services: YouTube, X, Facebook, Instagram, TikTok, Snapchat, Reddit, Twitch, Threads and Kick.[170] Services excluded from the scheme include (among others) Messenger Kids, WhatsApp, Kids Helpline, Google Classroom and YouTube Kids.[171] Gaming platforms such as Roblox are also excluded.

3.1.2 Content: What does the minimum age requirement entail?

The Australian minimum age prohibits the use of social media by users under the age of 16. However, it is important to note that there are no penalties for the users themselves; only for the regulated service providers. They are obliged to take reasonable steps to prevent users below the age limit from having an account on their platform.[172] Furthermore, under no circumstances may (digital) ID card data be collected, unless reasonable alternative assurance methods are also offered.[173] Under legislative rules, other types of data may also be excluded from collection.[174]

The age limit applies only to holding an account, and therefore not to the use of the regulated service *without* an account. The extent to which a service can be used without an account varies from case to case. On YouTube, for example, most content can be viewed without an account. Posting content or comments is impossible without an account, but passive viewing of content remains possible. On Instagram and Facebook, however, a relatively large amount of content is restricted.

In September 2025, the eSafety Commissioner published a Regulatory Guidance document, which, among other things, explains the requirement to take 'reasonable steps'.[175] To assess the effectiveness of various age assurance techniques, a test study was also conducted for this purpose: the Age Assurance Technology Trial.[176] The Regulatory Guidance discusses the effectiveness of various techniques and concludes that both age inference (based on observable behavioural patterns) and age estimation (based on biological characteristics such as the face) are technically feasible.[177] Age verification is also suitable, but, as indicated above, this is not legally permitted as the *sole* option for age verification. Collaboration with third-party age assurance services is permitted, but the responsibility for due diligence lies with the service provider.

168 https://minister.infrastructure.gov.au/wells/media-release/social-media-minimum-age-update-targets-harmful-tools
169 Online Safety (Age-Restricted Social Media Platforms) Rules 2025. www.legislation.gov.au/F2025L00889/latest/text
170 https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions/which-platforms-are-age-restricted
171 https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer
172 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Section 63(D): "must take reasonable steps to prevent age-restricted users from having accounts with the age-restricted social media platform".
173 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Section 63DB.
174 Online Safety Amendment (Social Media Minimum Age) Bill 2024, Section 63DA.
175 https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1760259175655.
176 https://ageassurance.com.au/report/.
177 https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1760259175655.

According to the eSafety Commissioner, given the current state of the art, the following indicators can in any case be taken into account:

Location-related signals:

- IP address
- GPS and other location data from the end device
- Language and time settings of the end device
- Device identifier of the end device
- Phone number
- App store/operating system/account settings
- Photos/tags/connections/engagement/activity

Age-related signals:

- Age of the account (e.g. the account has existed for 10 years or more)
- Interaction with content aimed at children or early teens
- Linguistic analysis/language processing indicating that the end user is likely a child
- Analysis of information/messages provided by the end-user (e.g. analysis of text indicating age)
- Visual content analysis (e.g. facial age analysis performed on photos and videos uploaded to the platform)
- Audio analysis (e.g. age estimation based on voice)
- Activity patterns consistent with school schedules
- Connections with other end-users who appear to be under 16
- Membership in youth-focused groups, forums or communities[178]

One key recommendation is successive validation, also known as the waterfall approach.[179] This involves combining various age verification techniques and applying them in stages, depending on the degree of certainty in a particular case. Margins of certainty, or buffer thresholds, can be used to separate certain cases from uncertain ones. For example, with a minimum age of 15, an age estimate of 21 or above can be accepted as definitive, whilst an estimate between 15 and 21 is subject to additional checks (e.g. human intervention or a biometric check). Depending on how these buffers are calibrated, the risk of false positives (unjustified acceptance of minors) and false negatives (unjustified rejection of adults) can be adjusted.

Furthermore, the report also sets out general principles for the assessment of reasonable measures:

- Reliability, accuracy, robustness and effectiveness
- Privacy preservation and data minimisation
- Accessibility, inclusivity and fairness
- Transparency
- Proportionality
- Evidence-based and responsive to new technological developments and risks[180]

Furthermore, when designing age verification measures, the best interests of the child must be paramount. These principles are then linked to more specific recommendations; in addition to the aforementioned waterfall method and buffer thresholds, for example, the use of audits and red teaming

178 https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1760259175655.
179 Ibid.
180 Ibid.

to test for potential circumvention methods; risk assessments based on the nature of the service; mitigating bias in international technologies developed in demographic contexts other than the Australian one; and transparently explaining policy measures to users and other target groups. In a later report, the eSafety Commissioner's view is summarised as follows:

> An assessment of reasonable steps is contextually dependent, requiring a review of both the regulatory landscape and business circumstances together. It is not a prescriptive test with a one-size-fits-all approach, but instead requires a review of all the steps taken in totality for an accurate and objective review of whether a platform has complied with the SMMA obligation.[181]

Additional guidance on privacy-related aspects is provided by the Office of the Australian Information Commissioner (OAIC).[182]

3.1.3 Supervision: How is compliance enforced?

Supervision of the minimum age requirement lies with the Australian eSafety Commissioner. In the event of breaches, they may impose a penalty of up to 50 million Australian dollars (~30 million euros). Since this is a best-efforts obligation, platforms are not directly liable for individual breaches by users. A penalty is only possible if the regulator demonstrates that reasonable steps to prevent underage use have not been taken:

> "It is not the intention that the Bill would punish a platform for individual instances where young people circumvent any reasonably appropriate measures put in place by the platform – however, a systemic failure to take action to limit such circumventions could give rise to a breach."[183]

To monitor effects, the eSafety Commissioner has announced a partnership with the Stanford University Social Media Lab. This research team leads an academic advisory board comprising 11 international experts in the field of child protection and social media, and is tasked with conducting long-term, large-scale research into the effects of the new policy.[184] Their intention is to publish findings regularly throughout 2026 and 2027. After two years, the first comprehensive evaluation of the legal framework will also take place.

181 eSafety Commissioner, 2026. Social Media Minimum Age: Compliance Update. (Hereinafter: 'eSafety Commissioner Compliance Update').https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806.

182 Office of the Australian Information Commissioner, 2025. Privacy Guidance on Part 4A (Social Media Minimum Age) of the Online Safety Act 2021.https://www.oaic.gov.au/privacy/privacy-legislation/related-legislation/social-media-minimum-age.

183 eSafety Commissioner, 2025. Social Media Minimum Age: Regulatory Guidance, p. 46, note 90.https://www.esafety.gov.au/sites/default/files/2025-09/eSafety-SMMA-Regulatory-Guidance.pdf?v=1760659200060.

184 https://www.esafety.gov.au/newsroom/media-releases/esafety-appoints-stanford-university-led-academic-advisory-group-to-assess-the-impacts-of-the-social-media-minimum-age-obligation.

3.1.4 Impact: What do we know about the results?

Much remains unclear regarding the implementation of the new minimum age in Australia – not only because of the short timeframe, but also because of the limited visibility of minors in their interactions with online platforms.[185]

Age assurance practices of regulated platforms

The most common age assurance method in practice is age estimation. More specifically, there is a combination of profiling-based age *inference* and biometric age *estimation*. Age inference involves analysing behavioural signals and other user data to estimate age.[186] Exactly which signals and methods platforms use is largely unknown.

It is, however, clear that some platforms, including TikTok, carry out biometric age estimation based on facial scans. The user is asked to activate the camera or webcam so that an age estimate can be made based on the image of their face. Not every user receives this request – only a subgroup that, based on inference, is deemed likely to be underage. Facial recognition is relatively accurate for younger children, and less reliable for teenagers close to the age limit.[187] Young people can also take steps to manipulate these scans, for example by using masks, make-up and other disguises; or simply by scanning an adult's face instead of their own.

Finally, some platforms also appear to accept the sharing of credit card or ID card details as a verification option. This is usually offered as an additional option, for example when the facial scan has failed. (As mentioned, Australian law prohibits platforms from using this as the sole verification method.) Platforms may also collaborate with independent service providers (third-party age assurance). Collaboration with Apple, for example, is possible via their Age Range API, which shares the age category of iPhone and Macbook users.[188] These devices can then be checked by parents to ensure they display the correct age.

In a recent report, the eSafety Commissioner identified a number of 'poor practices' among platforms that contribute to inadequate age verification:

1. Messaging to children aged under 16 on some platforms has encouraged them to attempt age assurance even where their declared age prior to 10 December 2025 was under 16.
2. In some cases, platforms have enabled children under the age of 16 to repeatedly attempt the same age verification method in order to ultimately obtain a 16+ result.
3. Pathways for reporting age-restricted accounts have generally not been accessible and effective, particularly for parents. [for example, through the use of deterring or misleading instructions; or by restricting access to third parties with their own user accounts]
4. Some platforms appear not to have done enough to prevent children aged under 16 from having accounts. However, eSafety is continuing its investigations to enable it to form a concluded view as to whether any platform has not taken reasonable steps to comply with the SMMA obligation.[189]

185 Rieder, B. & Hofmann, J., 2020. Towards platform observability. Internet Policy Review, 9(4).
186 eSafety Commissioner Compliance Update. ("Some platforms have chosen not to apply any age inference models for purposes of SMMA compliance (even where they have existing models in place), some are still working on rolling out age inference technology (in some cases, relying on very limited signals), and others have applied models which appear to take months, rather than weeks, to produce a high-confidence flag that the account may be held by a child aged under 16.")
187 eSafety Commissioner Compliance Update.
188 Ibid.
189 Ibid.

Impact on usage

In the first few days after the minimum age came into force, Meta says it deactivated approximately 550,000 user accounts belonging to minors.[190] By mid-December, according to the eSafety Commissioner, a total of approximately 4.6 million user accounts had been deactivated or deleted in compliance with the new minimum age.[191] In the period up to and including March, a further 310,000 accounts were dealt with.[192] These figures may seem high, yet they do not yet provide conclusive evidence that enforcement is actually effective (for example, due to the fact that deactivated users may well be able to create new accounts).[193] Anecdotal evidence also points to implementation issues; several media outlets have reported on teenagers who feel the new minimum age has had little effect.[194]

Surveys provide a clearer picture of compliance. A study by the eSafety Commissioner shows that the proportion of families with children aged between 8 and 15 who had a social media account fell from 49.7% to 31.3%—in other words, a reduction of 38%. A decline was observed across all 10 regulated platforms. For active young people with accounts on Facebook, Instagram, Snapchat and TikTok, the decline was smaller: around 7 out of 10 young people under 16 kept their accounts.[195] The eSafety Commissioner also notes differences between the verification measures of various platforms (although it does not name the platforms in question). The key data are shown below. An important caveat is that this data was reported by parents, not by the children themselves. It is therefore possible that the actual decline is even smaller, since some children may be keeping their activity secret from their parents.

190 https://www.pm.gov.au/media/4-7-million-accounts-deactivated-removed-or-restricted.
191 eSafety Commissioner Compliance Update.
192 Ibid.
193 A thorough analysis therefore requires a multi-year overview of reporting trends, with the ability to compare across multiple platforms. Reporting trends fluctuate, for example, depending on the season.https://www.crikey.com.au/2026/03/13/teens-social-media-ban-kids-still-using-platforms/.
194 Wilson, C. 2026. Most teens on social media pre-ban are still on those platforms, new data suggests. Crikey.https://www.crikey.com.au/2026/03/13/teens-social-media-ban-kids-still-using-platforms/.
195 eSafety Commissioner Compliance Update.

Table 1: The proportion of parents who reported that their child aged 8 to 15 years had their own social media account pre- and post-implementation of the social media age restrictions, by platform.

Age-restricted social media platform	% holding account(s) pre-implementation[a]	% holding account(s) post-implementation[b]
Facebook	13.8%	8.8%
Instagram	20.2%	13.9%
Kick	0.9%	0.2%
Reddit	2.5%	1.4%
Snapchat	27.3%	18.9%
Threads	1.4%	0.8%
TikTok	24.1%	16.7%
Twitch	2.6%	1.6%
X (Twitter)	1.8%	1.2%
YouTube	36.5%	17.7%
Any age-restricted social media platform	**49.7%**	**31.3%**

[a] **Source Q:** Thinking back to before the social media age restrictions came into effect (on 10 December 2025), did your child have their own account on the following social media platforms (i.e. an account in their own name)?

[b] **Source Q:** Does your child currently have their **own** account on the following social media platforms (that means an account in their own name)?

Base: Total sample (*n* = 898).

Screenshot taken from the eSafety March Compliance Report[196]

This survey also highlights behavioural changes among parents and young people. Participating families report that, in 36.3% of cases, the decision to stop using social media was initiated by the child themselves, and in 26.6% of cases by the parents themselves. 43.6% of cases involved account deletions initiated by the platform.[197]

Third-party research also points to non-compliance ranging between 60% and 70%, depending on (e.g.) the age group surveyed. A survey by the Courier-Mail published on 7 March 2026 concluded that 70% of the teenagers surveyed, aged between 10 and 16, were still active on social media.[198] The Molly Rose Foundation, on the other hand, concludes that 61% of Australian children aged between 12 and 15 who had an account prior to the law coming into force still have access to one or more accounts.[199] A pre-print academic paper by Leonardo Bursztyn *et al*. finds a non-compliance rate of 63.8% among 14- and 15-year-olds.[200] (With an

196 eSafety Commissioner Compliance Update.

197 Ibid, p. 14. (The Update does not expressly clarify how the total percentages reported here could exceed 100%, but presumably this is due to the fact that single family case may involve multiple deactivations across different accounts and social media platforms).

198 The Courier Mail, 'Teens Still on TikTok and Instagram Despite Ban', 7 March 2026. https://www.couriermail.com.au/education/support/technology-digital-safety/teens-still-on-tiktok-instagram-despite-ban-as-experts-reveal-simple-workarounds/news-story/d7c3ad5343a791d7816caf8a88c8a179

199 The Molly Rose Foundation, 2026. More than 60% of Australian children still using social media despite ban for under-16s, research shows.https://mollyrosefoundation.org/more-than-60-of-australian-children-still-using-social-media-despite-ban-for-under-16s-research-shows/.

200 Bursztyn, L., Handel, B., Jiménez-Durán, R., & Roth, C. (2023). When Product Markets Become Collective Traps: The Case of Social Media. SSRN Electronic Journal.https://doi.org/10.2139/ssrn.4597079. (The terminology used in this study may be confusing; here, 'compliance rates' refer to compliance by users who were previously active on social media. Users who were never active on social media are not included, although they also comply with the law. What is described as 'compliance rates' in this study is described in this current report as 'reduction effects': the proportion of active users who stopped using social media following

estimated usage of around 87% prior to the minimum age, this indicates a reduction of approximately 27%.) Non-compliance is higher among 15-year-olds (68.3%) than among 14-year-olds (57.1%).

The available data are therefore reasonably consistent; among active underage users, the minimum age appears to have brought about a reduction of approximately 20% to 30%. Differences between these studies are also related to the varying age groups studied; the eSafety Commissioner's survey concerns a younger group (8–15), with lower usage rates. The observed reduction effect (38%) appears to be slightly higher than in independent studies, possibly because compliance is likely to be higher among younger minors (for example, because younger users are more easily identified in age estimates, are less able to circumvent these systems, and/or are subject to stricter parental supervision). In any case, the figures do not differ so significantly between surveys as to suggest fundamentally different policy implications.

An important follow-up question is how these figures will develop in the coming months and years. As discussed earlier, social media use is a social phenomenon involving network effects and other interactions between users. Teenagers surveyed indicate that they would only be prepared to stop using social media if two-thirds of their peers were to do the same.[201] A cause for pessimism is that this tipping point is still a long way off; the current level could, in fact, perpetuate a vicious cycle, and in the long term even lead to even lower compliance. Conversely, there is cause for optimism in the fact that young users are, on average, much less active; it is to be expected that these upcoming generations, who have grown up below the minimum age, will also experience weaker network effects – and thus have less motivation to circumvent the ban. After all, these new cohorts have had fewer opportunities to build thick networks on, or strong bonds with, social media. However, the continued presence of adults on the platform may in turn exert a persistent intergenerational network effect (inter-cohort effects), which nevertheless draws minors back to social media.[202] Other factors that may still change include the age verification measures implemented by platforms (as discussed, the supervisory authority has already identified several areas for improvement) and the social norms among older people, young people and third parties. All in all, future compliance trends remain difficult to predict, and ongoing monitoring by the eSafety Commissioner and their research partners will be essential

the introduction of the minimum age. 'Non-compliance', on the other hand, describes the proportion of active underage users relative to all minors.)

201 Bursztyn, L., Handel, B., Jiménez-Durán, R., & Roth, C. (2023). When Product Markets Become Collective Traps: The Case of Social Media. SSRN Electronic Journal.https://doi.org/10.2139/ssrn.4597079.

202 Ibid.

3.2 France

France has put forward the first European legislative proposal for a minimum age for social media. A proposal was adopted as early as 2023, but was not implemented due to a conflict with EU law. In early 2026, the Assemblée Nationale adopted a new proposal, and the Senate responded on 29 March 2026 with an amended version. (In addition to these proposals, a new law on age verification by pornography platforms is also being developed, which is not covered further in this report.[203]) A compromise between the two versions is now being sought, with a view to implementation before September 2026. The three proposals are discussed chronologically below.

3.2.1 The Law of 7 July 2023

Scope

The Law of 7 July 2023 establishing a digital age of majority (*'à instaurer une majorité numérique'*) would prohibit the use of social media by children under the age of 15, unless consent has been given by a parent or guardian.

Social media is defined as 'any platform that enables end users to connect and communicate with one another, share content and discover other users and content across multiple devices, in particular through online conversations, messages, videos and recommendations.'[204] Exceptions apply to 'non-profit online encyclopaedias and non-profit educational or scientific guides'.[205] These limited exceptions mean the scope of application is potentially broader than in Australia, where (among other things) gaming, chat and healthcare services are explicitly excluded.

Key obligations

These services are subject to the obligation to 'refuse registration of minors under the age of fifteen, unless one of the persons exercising parental authority over the minor consents to such registration'.[206] For existing accounts, providers must 'obtain the express consent of one of the persons exercising parental authority over the minor as soon as possible'.[207] Furthermore, they must provide users under the age of 15 with certain information, including details of the risks associated with using the service and the content of the terms and conditions. A mechanism must also be provided to enable underage users to monitor the time they spend on the service. Parents are granted the right to request service providers to delete underage accounts.

To determine the age of users, providers must apply 'technical solutions' that comply with the frameworks set by ARCOM, the French platform regulator.[208]

203 LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. For a discussion, see: Galissaire, J., 2025. Mind the Gap: Age Assurance and the Limits of Enforcement under EU Law. Interface.https://www.interface-eu.org/publications/age-assurance-gap .

204 LOI n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (hereinafter: "Loi 2023-566"), Article 1.

205 Loi 2023-566, Article 4(III).

206 Loi 2023-566, Article 4(I).

207 Loi 2023-566, Article 4(I).

208 Loi 2023-566, Article 4(I).

Enforcement and implementation

Enforcement is the responsibility of ARCOM, the French platform regulator.[209] Violations may be punished with a fine of up to 1% of the provider's global turnover. Unlike the Australian law, no explicit standard is set for the margin of error afforded to providers.

As indicated above, this law has not been implemented. Implementation of the law required an implementing decree from the Council of State[210] and this has so far not been issued. The reason for this may be a conflict with EU law; the European Commission had indicated that this law may be in breach of the DSA and the country-of-origin principle. The French law has been referred to the European Commission via the TRIS procedure.[211]

The European Commission responded with a 'Detailed Opinion' in which it explains the potential conflict with EU law, followed by a response from the French government and a counter-response from the European Commission.[212] With regard to child protection, the European Commission states briefly that, for the country-of-origin principle, the grounds for exceptions relating to child protection may be invoked. However, with regard to the DSA, it notes that child protection and age limits are already harmonised at European level, through Articles 28, 34 and 35 (discussed in Chapter II.1).

The French response invokes the AVMSD, which allows Member States to adopt stricter measures than those prescribed by the Directive, and to which the DSA does not give effect.[213] However, in its counter-response, the European Commission refers to its analysis of the relationship between the AVMSD and the DSA (already discussed in Chapter II.2.2), which concludes that 'Member States are prevented from adopting national measures that would overlap or contradict the fully harmonising framework of the DSA'.[214] Furthermore, the French law does not aim to implement the AVMSD, and its scope of application is also broader: not only video platforms but also communication platforms in a broader sense are regulated, meaning the law goes further than the AVMSD permits. The then-European Commissioner Thierry Breton criticised France for procedural errors and called on the country to restart the procedure.[215] Following this, France withdrew its submission, and the EC closed the procedure.

3.2.2 The Assembly's proposal of 26 January 2026

The publication of the DSA Guidelines on child protection by the European Commission pointed towards a new opening; as discussed in Chapter II, the European Commission notes in this document that Article 28 of the DSA allows Member States to introduce national age restrictions for social media, within the limits of EU law. The related age verification obligations, however, remain harmonised at European level by the DSA.

The National Assembly invoked this principle to undertake a renewed attempt at passing a minimum age.[216] An initiative proposal dated 26 November 2025 was adopted by the Assembly on 26 January 2026 following several amendments. The bill acknowledges that a European solution is needed in the long

209 Loi 2023-566, Article 4(II).
210 Loi 2023-566, Article 4(IV).
211 https://technical-regulation-information-system.ec.europa.eu/en/notification/24221.
212 Ibid.
213 DSA, Article 2.
214 https://technical-regulation-information-system.ec.europa.eu/en/notification/24221.
215 Galissaire, J., 2025. Mind the Gap: Age Assurance and the Limits of Enforcement under EU Law. Interface.https://www.interface-eu.org/publications/age-assurance-gap.
216 Assembléé Nationale, Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, n° 2107, déposée le mardi 18 novembre 2025 (Hereinafter: 'Proposition de loi, n° 2107'). https://www.assemblee-nationale.fr/dyn/17/textes/l17b2107_proposition-loi# ("However, the publication on 14 July 2025 of the European Commission's guidelines on the protection of minors under the Digital Services Act marks a significant shift in the European Commission's position and paves the way for national legislation on the age limit for access to social networks.")

term, but that the urgency of this issue would now compel France to act. In addition to a minimum age, this proposal also includes new measures relating to awareness-raising, smartphone restrictions in schools, and a digital curfew.

Broadly speaking, this proposal is similar to the previous one. Once again, social media (*réseaux sociaux*) is the target of regulation, with the same exemption for educational services. Once again, there is an obligation to refuse registration to minors under the age of 15 and to delete existing accounts belonging to that age group. Age verification techniques must comply with the frameworks set by ARCOM. The main difference is that the minimum age is unconditional this time; parental consent does not provide an exception.

For young people aged between 15 and 18, a 'curfew' is also being introduced; for all minors, accounts must be automatically deactivated between 22:00 and 08:00. To this end, the same age assurance technique must be used as for the minimum age. The aim of this rule is to 'limit screen time during rest periods and protect teenagers' sleep'.[217] The intention is also to create a 'consistent framework for all parents', 'facilitating the supervision of their children's digital activities'.[218]

3.2.3 The amended Senate proposal of 29 March 2026

An amended Senate proposal introduces several significant changes. Firstly, the minimum age is no longer formulated as an obligation for platforms, but as a ban directed at minors. Secondly, the ban does not apply to all social media, but only to those that may harm the physical, mental or moral development of minors.[219] For all other social media platforms, parental consent is still required.[220] A list of harmful social media platforms, to which the total ban applies, is drawn up by the Minister, following advice from the platform regulator ARCOM.[221]

The explanatory memorandum states that these amendments serve two purposes. Firstly, the earlier proposal was deemed too broad, as it regulated all social networks, "including purely collaborative and educational networks, some of which are used daily in a school environment and pose no particular risk".[222] According to an opinion from the Council of State, the proposal would even risk being unconstitutional, due to a possible violation of the Rights of the Child and of freedoms of communication.[223] Secondly, the role of parents is not taken into account, which, according to French civil law, "includes, amongst other things, guiding the child in the exercise of their fundamental rights and involving them in decisions concerning them".[224]

217 Proposition de loi, n° 2107, Articles 6–10.
218 Proposition de loi, n° 2107, Preamble.
219 Le Sénat, Proposition de loi n° 304, Protéger les mineurs des risques des réseaux sociaux, (hereinafter: 'Proposition de loi, n° 304', Article 6-9.I.https://www.senat.fr/amendements/commissions/2025-2026/304/Amdt_COM-4.html.
220 Proposition de loi, n° 304, Article 6-9.Ibis.
221 Proposition de loi, n° 304, Article 6-9.I.
222 Proposition de loi, n° 2107, Preamble.
223 Ibid.
224 Ibid.

3.2.4 Discussion

Following these two competing proposals, we now await a compromise between the National Assembly and the Senate. In any case, the following features of French policy are already worth noting:

1. **A focus on unsafe services:** Unlike the Australian legislature, the French Senate does not seek to impose a categorical minimum age for all social media. Only specific unsafe services fall within this framework.

2. **A tiered approach with a role for parental consent:** Related to this is the use of parental consent; alongside the absolute age limit for unsafe services, parental consent serves as a lighter safeguard for safe services.

3. **A curfew as a supplementary safeguard**, which applies to all users under the age of 18.

4. **Potential conflicts with fundamental rights:** The Council of State's advice identifies potential conflicts with fundamental rights, including the rights of the child, which necessitate a more layered and risk-based approach (as in the Senate proposal). Although this advice does not draw definitive conclusions about the role of fundamental rights in this area, it does point to potential tensions in the event of a categorical ban.

5. **Potential conflicts with European (internal market) law:** The French trajectory illustrates that the powers of national legislators in this area are limited. Legal exceptions may be invoked in relation to the country-of-origin principle, but these are burdensome. The recent Guidelines point to possibilities under the DSA, with enforcement concentrated at EU level under the DSA. It is noteworthy that the recent Senate proposal reformulates the standard to focus on young people, rather than platform providers. This may be an attempt to avoid conflict with EU platform law.

In other respects, however, the Senate's proposal still appears to interfere with platform regulation, for example by granting ARCOM powers regarding age verification standards, and the Minister powers regarding the assessment of safety on social media. This may result in an overlap with the powers of the European Commission and other DSA supervisory authorities, which may already have jurisdiction under Article 28 of the DSA. In the current Senate proposal, a conflict with EU law therefore still appears possible.[225] Implications for Dutch policy are discussed in Chapter IV.

225 Also relevant here is the European Commission's recent Recommendation on age verification, which reiterates and further clarifies its interpretation of the Guidelines: "As stated in the Guidelines, Members States may introduce national laws which, in compliance with Union law, prescribe a minimum age to access certain products or services offered and/or displayed in any way on an online platform. However, such national measures cannot impose additional obligations on online platforms, including age verification obligations, as it would undermine the full harmonisation effect of Regulation (EU) 2022/2065, given that the objectives of such measures would overlap with those already pursued by that Regulation". Commission Recommendation of 29 April 2026 on establishing a common framework for EU-wide Age Verification technologies. C(2026) 4225 final.https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies.

4 Scenarios and recommendations

This chapter sets out the options for implementing the government's policy on a European minimum age for unsafe social media. This discussion is divided into two sections: (1) substantive considerations, relating to the design of the age standard and the associated verification obligations; and (2) legislative and procedural scenarios, relating to the legal and regulatory framework within which the new policy is to be implemented.

4.1 Substantive considerations and recommendations

The foregoing demonstrates that a minimum age rule may differ in at least (1) the scope of application for different services, (2) the level of the age limit and associated restrictions, and (3) the age assurance obligations for platforms and any third parties. Below, we discuss the advantages and disadvantages.

4.1.1 Scope

In terms of service categories, the first question is how social media is defined, and what exceptions, if any, still apply. Subsequently, the obligation may apply to all social media (categorically), or only to social media that is insufficiently secure (risk-based).

"Social media" and/or other categories

For a definition of social media, one can refer to the definition of online social networking services in the Digital Markets Act (DMA), which is also adopted in the French model:

> "online social networking service" means a platform that enables end users to connect and communicate with each other, share content and discover other users and content across multiple devices and, in particular, via chats, posts, videos and recommendations.[226]

This definition is narrower than that of 'online platforms' in the DSA. Other types of services that facilitate the public exchange of user-generated content, such as marketplaces, also fall under the DSA definition, but are not online social networking services.

A comprehensive review of social networking services would go beyond the scope of this report, but based on recent enforcement actions by the European Commission, TikTok, Facebook, Instagram and LinkedIn are deemed to fall into this category.[227] In our view, it likely also applies to Snapchat, X, Reddit and YouTube.[228]

A follow-up question is whether the minimum age should also provide for exceptions for certain subcategories. The French Council of State concludes that educational platforms should be exempted, and

226 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act or 'DMA'), Art 2(7).

227 The DMA is an example of asymmetric regulation. This means that the substantive rules of the DMA are designed to apply to social networking services (and other core platform services) offered by large and influential gatekeepers, which are designated as such by the European Commission if they fulfil a gatekeeper function in the relevant market. On this basis, four social networking services have so far been designated and regulated by the European Commission, namely: TikTok, Facebook, Instagram and LinkedIn. However, the fact that other services are missing from this list does not mean that they fall outside the category of 'social networking services'. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.

228 YouTube has been designated as a video-sharing platform service in DMA enforcement, and not as an online social networking service. This does not, however, rule out the possibility that this platform could meet both definitions, and in other contexts (such as the French proposal) could indeed be regulated as a social networking service.

that this is even necessary to respect fundamental rights and the rights of the child.[229] In Australian law, the exceptions are even broader, but a direct comparison is not valid because the original definition is also broader.[230] It is striking, however, that Australia also permits additional exceptions by legislative rule (i.e. without amending the law). The Minister may implement such an addition if "the Minister is satisfied that it is reasonably necessary to do so in order to minimise harm to age-restricted users".[231]

Based on the definition in the DMA, it is likely that chat services such as WhatsApp, Telegram and Discord, as well as gaming services such as Roblox, will fall out of scope.[232] However, this depends on the circumstances of each case, and the extent to which these services also incorporate social features (such as live streaming or semi-public pages). From a policy perspective, too, it is debatable whether these services should be subject to the same minimum age rule. A comprehensive analysis is beyond the scope of this report. An earlier academic report concluded that gaming and chat pose relatively lower risks, and would therefore justify a lower minimum age of 13 rather than the higher threshold of 15 for social media.[233] A potential ban on social media for young people could also lead to spillover effects, with young users turning to unregulated alternatives. (According to the Australian regulator, however, such a spillover effect is not yet noticeable in practice.[234]) In principle, the DSA already provides broad and flexible frameworks for regulating these different types of services within the broader category of 'online platforms' (see also IV.2 below). To that extent, it seems justifiable to prioritise social networking services in the short term.

There is no doubt that some services pose significantly higher risks than social media, such as gambling and pornography platforms. The EU already has stricter age verification requirements for such services, but enforcement remains a concern. The European Commission has now taken initial steps against very large pornography platforms falling within its jurisdiction, but Member States also have a role to play in supervising smaller pornography services and other high-risk services established in their countries. A new policy for social media should therefore be accompanied by a continued focus on the enforcement of existing obligations for high-risk services such as pornography and gambling websites (without prejudice to the independence of the ACM as the primary regulator in this area). If the minimum age for social media were to receive the full focus of attention now, whilst most pornography platforms do not meaningfully check users' ages, the policy could lose its legal (and social) persuasiveness.

> **Recommendation A1:** *For the definition of social media, alignment could be sought with the concept of 'online social networking service' from the Digital Markets Act.*
>
> **Recommendation A2:** *Allow leeway for introducing additions and exceptions to the minimum age via secondary legislation (for example, for educational platforms), based on changing market factors, societal conditions and other developments.*
>
> **Recommendation A3:** *Ensure that the focus on social media does not come at the expense of, but rather goes hand in hand with, the supervision and enforcement of age verification for higher-risk services such as pornography and gambling platforms.*

229 See Chapter III.2.
230 Chat and calling services, gaming, professional networks and educational platforms, among others, are exempt. See Chapter III.1.1.
231 Online Safety Amendment (Social Media Minimum Age) Bill 2024, 63C4.
232 Although the DMA definition does refer to 'chats', chat services generally do not meet the other requirements, such as the sharing or discovery of content. The precise implementation, however, varies by service.
233 Koning, I. et al., 2025. Guidelines on Healthy Screen Use. Ministry of Health, Welfare and Sport. https://www.rijksoverheid.nl/documenten/rapporten/2025/06/17/richtlijn-gezond-schermgebruik-2025.
234 eSafety Commissioner, March Compliance Update.

Restriction to "insufficiently safe" social media

The coalition agreement aims for a minimum age "as long as social media are insufficiently safe". This condition is open to multiple interpretations. On the one hand, it may imply that all social media are deemed insufficiently safe, at least under current circumstances. On the other hand, it may also suggest a case-by-case assessment, whereby the minimum age may apply to certain (unsafe) social media platforms but not to others.

Whether social media should be regarded as inherently unsafe requires a scientific assessment of the existing risks, but also a political judgement as to which risks are acceptable. This judgement involves a determination as to what level of safety is 'sufficient', weighed against the potential benefits offered by social media and the other implementation costs and restrictions on fundamental rights associated with a minimum age.

Scientific basis for the safety assessment

At a scientific level, there is growing evidence of the potential harmful effects of social media.[235] At the same time, critical experts emphasise that convincing causal evidence regarding the negative effects on mental health is limited, and also point to the positive correlations of social media for certain groups.[236] Moreover, the negative correlations with social media appear to be heavily concentrated among the relatively small group of young people who exhibit excessive use, which could call into question the proportionality of a general ban. Limiting usage time, possibly also for adults, might be a more proportionate alternative.

As discussed in Chapter II.5.4, however, a minimum age does not necessarily (or exclusively) need to be based on causal evidence of mental health effects. Firstly, social media is also associated with various forms of exploitation and abuse ('online harms'). Although platforms also have obligations to prevent such abuse, it has proved challenging in recent years to persuade platforms to take effective action. Secondly, many young people also indicate that they are dissatisfied with their own use of social media.[237] More generally, under prevailing interpretations of the Convention on the Rights of the Child, a precautionary principle applies to justify preventive action.[238] In other aspects of media policy and child protection too – for example, restrictions on pornography – action is not taken solely on the basis of conclusive scientific evidence of causality.

Advantages of a categorical approach

On such grounds, the Australian government has already concluded that social media are inherently unsafe and has introduced a categorical minimum age for all social media.[239] This approach has the advantage of consistency and predictability. Under the risk-based approach, by contrast, the government incurs an important task in monitoring platforms and assessing their safety. Monitoring the risk assessments of platforms is challenging and costly, partly due to the novelty and complexity of this field, and the significant information asymmetries in platform supervision.[240] In practice, this monitoring can also lead to delays and legal uncertainty. By avoiding these pitfalls, the categorical minimum age guarantees an equal level of protection across all social media in the short term.

235 Chapter II.5.4.
236 Ibid.
237 Ibid.
238 Ibid.
239 Chapter III.1.
240 Rieder, B. & Hofmann, J., 2020. Towards platform observability. Internet Policy Review, 9(4), pp.1–28. Terzis, P., Veale, M. & Gaumann, N., 2024. 'Law and the Emerging Political Economy of Algorithmic Audits', Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency.https://dl.acm.org/doi/10.1145/3630106.3658970.

Advantages of a risk-based approach

Although a risk-based approach offers less clarity, it has the advantage of helping to maintain proportionality; the minimum age can be targeted at the services where it is most necessary, without imposing excessive restrictions on safer services. This increases the likelihood that a minimum age would withstand a constitutional review.

Another important advantage of a risk-based approach is that it can encourage platforms to continue investing in other child protection measures. A common criticism of categorical minimum age policies is that they would discourage platforms from effectively protecting children on their service; after all, children are expected not to be present in the first place. On paper, such obligations can coexist, but in practice there are inevitable tensions between prohibiting and improving young people's user experience. Under a minimum age, it is likely that platforms will have less scope to develop safe and attractive features for children, as any children present will likely take steps to conceal their true age from the platform. Monitoring children's user experiences can therefore become challenging; by definition, it concerns a user group that the platform has been unable to identify as such. In communications with regulators and third parties, platforms also face a similar tension between (sharing information about) prohibiting underage users and improving their experiences.

Under a risk-based approach, the minimum age actually serves as an incentive to provide an adequate level of protection. If the platform can demonstrate that it is sufficiently safe, it is effectively 'rewarded' with the privilege of being allowed to admit children to its service. (The same objective could perhaps also be achieved through tiered age limits, discussed below).

Current law

Our analysis shows that EU law already reflects a risk-based interpretation of the coalition agreement. Most social media platforms already apply a contractual minimum age of 13, and in principle a higher mandatory minimum age may apply to services with a high risk that is not sufficiently mitigated by other protective measures. To date, the Commission has not seen grounds to require such a higher mandatory age for social media. In most cases, the GDPR also appears to require parental consent up to the age of 16 (at least in the Netherlands).

A possible middle ground, alongside the statutory establishment of a categorical minimum age, is to adjust the relevant burdens of proof. This could be achieved, for example, by specifying in law that the competent supervisory authority under the DSA may prescribe a minimum age and/or certain assurance obligations as a measure in the case of platforms that are not sufficiently secure. Assessment criteria for this safety test could also be laid down. Under the current framework, these aspects are not explicitly regulated by law, but only in the subordinate Guidelines, and the platform also appears to retain a degree of discretion in selecting the appropriate measures. Naturally, this would be a relatively minor intervention, which merely aims to clarify the current law.

Should a risk-based approach be preferred over a categorical one, it is in any case advisable not to duplicate the current risk assessment framework from the DSA, but to build explicitly upon it. Risk assessment is a complex process that requires considerable resources and expertise not only from platforms but also from supervisory authorities. Such efforts are already being made under the DSA. For the purposes of applying a minimum age, it would therefore be inefficient to entrust the safety assessment to a different supervisory authority.

Policy option B1: *The minimum age could apply to all social media (categorical), or only to unsafe social media (risk-based). The categorical approach offers legal certainty and short-term feasibility, whilst the risk-based approach is more proportionate in relation to fundamental rights and encourages platforms to continue investing in other forms of child protection.*

Recommendation B1: *The second option requires a risk assessment framework to determine which social media platforms are sufficiently safe for minors. To this end, the current risk assessments under Article 28 of the DSA provide a valuable starting point. Future amendments could potentially modify this framework, e.g. by adjusting risk thresholds or burdens of proof, in order to help to enforce a mandatory minimum age more quickly and widely.*

4.1.2 Age limit

What age?

The Australian minimum age of 16 is relatively high compared to similar proposals in Europe. Discussions are currently underway in Europe regarding a lower age limit of 15, which is also in line with earlier recommendations by State Secretary Karremans based on the 2025 Healthy Screen Use Directive.[241] Based on this Directive, it was recommended that smartphone use should, in principle, not be permitted before the age of 11; social interaction platforms and messaging services, such as WhatsApp and Signal, not before the age of 13; and social media such as TikTok, Instagram and Snapchat from the age of 15.[242]

Binary or tiered age groups?

Another option worth considering is a tiered age limit, whereby some services or features are made available earlier than others. This would allow young users to go through a transitional phase, enabling them to familiarise themselves with social media in a relatively safe environment. With binary age limits such as the Australian one, there is now a concern that young people are not given the chance to develop skills and resilience before they suddenly gain access to a relatively unsafe environment on their 16th birthday. With a tiered age limit, platforms could apply safety by design and default to give users aged between 13 and 15 access to a safe version of the platform. In this safer version, certain risky features could be restricted for underage users, or switched from opt-out to opt-in ('*by default*'). Such principles of *safety by design* are already recommended as best practices in (among other instruments) the Guidelines and the Online Safety Code.

A tiered age limit could also create an incentive for platforms to continue investing in child safety. As discussed above, a categorical minimum age may actually introduce a tension between banning and improving usage among young people. A tiered age limit might help to reduce this tension between improving and banning. After all, the platform retains a responsibility for the protection of 13- to 15-year-olds on its service, and the measures it takes to this end may also have indirect benefits for the experience of younger users who circumvent the binding minimum age. Measures that apply by default would, in principle, also be designed to protect this group.

Under current EU law, a form of tiered protection already applies through the combination of different legal frameworks: most platforms impose a contractual minimum age of 13 (which they are required to enforce effectively under the DSA); the GDPR mandates parental consent up to the age of 16; and for pornography platforms and other high-risk services, a binding minimum age of 18 is, in principle,

241 https://www.rijksoverheid.nl/actueel/nieuws/2025/06/16/duidelijk-advies-voor-ouders-wacht-met-sociale-media-tot-15-jaar.
242 https://open.overheid.nl/documenten/db3c3c1f-5a3c-4a7b-9bf4-696a61d8ee2b/file (For smartphone use, the guideline is 'Year 8' of Dutch primary school; most pupils are at least 11 years old by then. For that age group, 'practising with a smartphone under parental supervision' still falls within the scope of the advice.)

mandatory. Any legislative amendment could maintain this system; or possibly clarify it and address other preconditions such as age verification and enforcement; or, conversely, replace it with a binary minimum age. The features of the safe service version could also be specified, such as a usage time limit or a curfew.

> **Recommendation C1:** *Consider applying a tiered age limit, whereby access to the service is denied only to users under the age of 13, and young people aged 13 to 15 are granted access to a safe version of the regulated service. Specific features of the safe version could also be prescribed, such as a usage time limit or a curfew.*

4.1.3 Age assurance and feasibility

Enforcing a minimum age requires the cooperation of platforms (and possibly third parties). Under the heading of 'age assurance', platforms can employ various techniques to verify the age of their users. Selecting the appropriate technique involves a trade-off between effectiveness and intrusiveness. Self-declaration alone is the least intrusive but also the least effective approach; there is now a consensus that self-declaration has little or no effect on compliance. More intrusive and effective are age estimation and facial scans. Perhaps even more intrusive and effective is age verification based on ID cards, bank details or similar age documentation. However, the potential restriction on fundamental rights such as privacy increases with these measures. Age estimation is often positioned as an intermediate solution, but can be equally intrusive to user privacy, particularly when involving extensive profiling and/or biometrics.[243] Circumvention remains possible in all cases, particularly through the use of VPNs or by enlisting the help of adults.

Age estimation and facial recognition

The Australian case offers many insights into age estimation and facial recognition, as most platforms have opted for a combination of these methods.

The available data suggests that this approach, whilst more effective than self-declaration alone, yields modest results; as discussed above, these measures appear to be flawed in that approximately 60% to 70% of underage teenagers remain active on social media despite the minimum age requirement. The planned study by Stanford University, in collaboration with the eSafety Commissioner, is expected to provide more detailed insights. The Australian regulator has identified several poor practices from platforms that may undermine the current implementation.

Cultural changes may also shape compliance in the longer term. For example, it seems plausible that the current generation of minors, who are already accustomed to using social media and have invested time in building a profile and network, feel a stronger motivation to circumvent age verification than future generations growing up under the new minimum age. Network effects can create tipping points that cause relatively sudden shifts in behaviour. It remains difficult to predict what other effects might arise in the long term.

In the short term, it is likely that these methods will be far from foolproof; an effectiveness rate of 30% or even lower is also to be expected in the Netherlands. This may also have legal implications when assessing proportionality, in the event of significant interference with fundamental rights resulting from imposed obligations.

243 See footnotes 24 and 26 above. Shaffique, M. & van der Hof, S., 2026. Behavioural profiling for age assurance: do the ends justify the means?, International Data Privacy Law, 16(1),https://doi.org/10.1093/idpl/ipaf012.

Compared to Australia, stricter privacy safeguards apply in Europe under the GDPR and DSA. Under the current European legal framework, it remains unclear whether and to what extent the same age estimation methods are permissible. The DSA now stipulates that platforms are not obliged to store additional information to determine the user's age, and service providers are therefore limited to using data that is already being collected on other grounds. The GDPR also sets limits on (among other things) the purpose limitation and proportionality of processing. It therefore remains unclear in advance what options remain, and these options may also vary from platform to platform. A legislative amendment could potentially adjust these frameworks to permit more intrusive forms of profiling and verification. However, this could run counter to the intention set out in Article 28(3) of the DSA and Article 11 of the GDPR that age verification should not drive an expansion of platform surveillance and profiling, and is potentially at odds with the constitutional principle of proportionality. Unless there is a specific reason to mandate a particular estimation method—for example, due to a demonstrably high degree of effectiveness and proportionality—caution is therefore required when expanding user profiling.

Age verification

Age verification, by means of documentation such as ID cards or bank details, is a more intrusive alternative, which is treated differently in various legal systems.

In Australia, requesting ID details is actually prohibited unless the platform also offers alternative methods. As part of the 'waterfall' method of successive validation, platforms may, for example, make age verification mandatory if a user has failed the age estimation; it then effectively functions like an appeal mechanism.

In the EU, the European Commission, as the DSA supervisory authority, is pushing relatively hard for age verification as a mandatory measure, if not for all social media then for higher-risk services such as pornography platforms. Work is also underway on industry standards for effective and privacy-friendly age verification; in the long term via the European Identity Wallet and in the shorter term with the EU Age Verification App, alongside related pilot projects in several Member States. The European Commission is now encouraging all Member States to develop their own app in compatibility with the EU Age Verification App.[244] However, there is persistent criticism regarding the readiness of this EU solution, and more generally regarding the proportionality of verification requirements.

Although age verification technology is making progress, as a legal requirement it remains experimental, poses a risk to fundamental rights, and may be costly to implement. Verification restricts not only the freedom of minors but of all users who are obliged to participate in this process. Moreover, age verification is still far from foolproof: circumvention through the use of VPNs or with the help of adults remains relatively straightforward in most cases, even for young people.

Given the high costs, including risks to fundamental rights, and given the limited effectiveness, the proportionality of a mandatory verification requirement is therefore open to question. To help address these concerns, possible safeguards include organising alternative (possibly physical) verification methods for vulnerable groups, and not introducing the verification requirement universally but focusing it on specific scenarios (including a risk-based age policy, and/or successive validation or the 'waterfall method').

244 The introduction of this app may also require legislative changes at national level, for example to ensure compliance with the GDPR. This report does not consider this issue further.

Standard-setting and the role of parents and third parties

In addition to the platform, others can also be held accountable for their responsibilities and potential role. Most importantly, parents and children themselves can be encouraged to deactivate accounts. However, most current proposals choose not to impose sanctions on these parties. Lawmaking can however contribute to articulating social norms and expectations; it is easy to imagine that a parent might be more willing to ban social media for their child if this norm were also prescribed by law—and that child might be more easily persuaded. In the Australian context, such norm-setting effects appear to be significant: since the minimum age requirement came into force, more than half of deactivations have been initiated by parents and young people themselves, not by the platform.[245]

Policy measures to support the establishment of norms merit further investigation. Firstly, effective communication of expectations can play a role. In addition to parents, schools, for example, could also play a role in encouraging compliance. Effective *parental controls* on the device are of vital importance to parents. Most operating systems (macOS, iOS, Windows, Android, ChromeOS) already offer systems that enable parents to set the user's age and to grant or withdraw permission to use certain apps. These systems can be highly effective, but do require awareness and digital literacy on the part of parents. Schools, libraries and/or other public institutions may have a role to play in supporting parents in making effective use of these tools.

Since the private sector already offers effective solutions, it does not appear necessary at this stage to prioritise, as a regulatory matter, the development of parental controls in user devices or related software products. However, this conclusion remains conditional, and the government may in any case play a role in encouraging self-regulation in this space. In some circumstances, these solutions also depend on interoperability with the platform service. Ideally, therefore, as part of the DSA's risk management framework, platforms can be expected, where appropriate, to ensure interoperability with available parental controls.[246]

Other authors have also proposed so-called *nudges* that could promote compliance, such as proactively making alternative activities available or subsidising them.[247] These subsidies could potentially also be provided in the form of vouchers for young people as a reward for verified compliance with the minimum age. These ideas are experimental – it remains unclear, for example, how compliance can be verified – but they also merit further exploration.

245 See Chapter III.1.https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf?v=1774905032806.

246 See also the recommendations of the Australian regulator regarding, among other things, interoperability with the Apple Age Range API (Chapter III.1.4). Similar principles apply under the DSA.

247 Bursztyn, L., Handel, B., Jiménez-Durán, R., & Roth, C. (2023). When Product Markets Become Collective Traps: The Case of Social Media. SSRN Electronic Journal.https://doi.org/10.2139/ssrn.4597079.

Recommendation D1: *With any (proportional) approach to age verification, circumvention remains possible. Policymakers should therefore anticipate significant non-compliance*.

Recommendation D2: *Age verification entails privacy risks. The relevant frameworks must also provide explicit safeguards for the effective protection of privacy and data protection.*

Recommendation D3: *Australia's experience with age estimation has yielded useful insights into best and worst practices for age estimation, which are also applicable in European contexts. These standards can serve as a source of inspiration when developing European policy, within the limits of the GDPR's privacy safeguards under EU law.*

Recommendation D4: *Age verification may, in theory, offer the most accurate assurance, but it also poses some of the greatest privacy risks and entails the highest implementation costs; moreover, it remains vulnerable to circumvention. Consequently, a mandatory age verification requirement for social media may be disproportionate in relation to users' fundamental rights to privacy and freedom of information.*

Recommendation D5: *Given the limited effectiveness of age assurance, appeals can also be made to the responsibility of parents and minors themselves. Parental controls in peripheral devices, and support from institutions such as schools and libraries, can assist parents in this role.*

4.2 Legislative scenarios

A minimum age for social media can be introduced using various legislative methods. Which option is most suitable depends in part on substantive considerations. Below, we discuss options at national and EU level.

4.2.1 Enforcement of existing frameworks

Chapter II has shown that the current legal framework offers a high level of protection for young people—at least on paper. Although enforcement has long been sparse, the European Commission has in the past year taken significant steps to enforce child protection rules in general, and age verification rules in particular.

The following requirements are clear: under the DSA, platforms must enforce their standard contractual minimum age of 13, and, under the GDPR, ensure parental consent for users under 16. For pornography platforms, a mandatory minimum age of 18 applies. On the basis of a risk assessment tailored to a specific service, the DSA regulator could, in theory, also deem a statutory minimum age necessary and/or mandate other additional protective measures, such as a curfew or a limit on usage time. Viewed in this light, it can therefore be argued that current EU law already meets the ambitions set out in the coalition agreement; the main focus ought then to lie on enforcement.

However, the contractual minimum age of 13 is relatively low, and the parental consent rules under the GDPR are unclear on several points and, moreover, may be dependent on enforcement by independent national authorities. The European Commission may address these shortcomings by mandating additional measures through the risk assessments in the DSA. However, the precise requirements of this risk assessment remain difficult to predict in practice, leaving a significant role to the European Commission as the primary regulator in this area. In any case, a categorical minimum age for all social media is not an option; the risk-based approach requires a case-by-case assessment, in which the platform also has a degree of discretion to select appropriate measures. The European Commission therefore faces a relatively high burden of proof in enforcing minimum ages as a protective measure. Platforms can also challenge

these assessments individually, which further increases the duration and uncertainty of this approach. The current risk-based framework thus offers nuanced, tailored solutions, but risks causing delays and uncertainty (see also IV.1.1). Conversely, a risk-based approach does represent a significant accommodation for fundamental rights concerns.

The current framework offers few opportunities for the Dutch government to directly influence enforcement. The European Commission and national supervisory authorities under the DSA and the GDPR are independent in their enforcement duties, and there is no formal mechanism to enforce or steer enforcement. Where the Dutch government can direct its efforts instead, is toward raising awareness and digital literacy (see also Chapter IV.I.3 under 'Standard-setting and the role of parents and third parties'). The Australian case study has shown the extent to which parents and minors themselves play a role in compliance with the minimum age. In particular, when it comes to using device-based parental controls, parents could be given even better support, for example by schools, libraries or other public institutions. Moreover, in the Netherlands there appears to be little awareness of the minimum ages that already apply under the General Terms and Conditions, the GDPR and the DSA. Through informative and proactive policies aimed at parents and young people, the Dutch government can still provide an important complement to the European Commission's platform-focused supervision.

4.2.2 Legislative changes at national level with European DSA enforcement ('the French model')

Many Member States are currently working on national legislation to introduce a national minimum age. France's proposals are the most advanced, but similar plans exist in Spain, Denmark, Greece and many other EU Member States, amongst others.

However, Member States' powers to regulate social media are limited, as this area is largely harmonised at EU level. As discussed in Chapter III.2, the country of origin principle also applies here, meaning that, in principle, only the country of establishment is competent to regulate online services established there.

The solution in the French Senate proposal is to focus the minimum age primarily on the behaviour of young people—not on platforms. In this way, a direct conflict with EU platform law can be avoided. This approach is also reflected in other parts of the DSA, and is accepted by the European Commission in its Guidelines. Under this approach, a Member State may determine what constitutes illegal user behaviour, but the responsibilities of online services regarding this behaviour remain harmonised at EU level.[248] Member States thus set their own minimum age for young people, and the European Commission and DSA regulators oversee *the* effective *implementation* of that age by platforms.

Incidentally, this approach appears not to have been implemented consistently in the current French proposal, as it still contains other provisions, including those on age verification, which are indeed directed at the platform. Another potential objection is that no sanctions are envisaged for young people when they breach the minimum age. In our view, however, this is not a fundamental objection and we do not encourage an approach in which sanctions would also apply to minors themselves.

Under national legislation, the TRIS applies to national measures concerning rules on information society services, so that the European Commission can assess their compatibility with EU law.[249]

As with the previous scenario, the influence of the Dutch government remains limited in this model. The

248 DSA, recital 12. See also: M. Husovec (2024). Principles of the Digital Services Act. Oxford University Press. As discussed in Chapter III.2, there are still elements from the French model that do appear to be targeted specifically at platforms, and may therefore give rise to tensions with EU law. A Dutch variant could, depending in part on future legal developments, consider focusing national legislation even more clearly on the obligations of young people.

249 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 on the notification procedure for technical regulations and rules on information society services. See the reference in the Guidelines in Chapter II.1 of this report.

minimum age itself is determined at national level, but many important enforcement decisions regarding (among other things) age verification remain in the hands of independent regulators and the European Commission. It is also relevant here that the Guidelines apply a relatively strict interpretation to the enforcement of national minimum ages: here, as with pornography platforms and other high-risk services, *verification* is, in principle, mandatory. However, as discussed in Chapter IV.1.3, there are serious fundamental rights risks associated with this approach. The Guidelines currently appear to leave little scope for a more layered and proportionate approach on this point.

An unexpected side effect of the French model is that it may actually strengthen supervision at European level. As discussed in Chapter II.2, there is currently an overlap of powers between the DSA and GDPR supervisory authorities regarding age standards, in which the European Commission may lack enforcement powers for the rules on parental consent under the GDPR as regards social media, which currently constitute the main protection for users aged between 13 and 16. If a similar parental consent requirement for social media were to be enacted as a standalone standard in national legislation (whether or not combined with a binding minimum age for unsafe services, as in France), the European Commission could also include this rule more straightforwardly in its supervision of platforms under the DSA. This could facilitate more effective enforcement; powers would be consolidated with the most active regulator in this field. The Commission must then, however, take into account differing standards across Member States.

4.2.3 Legislative change at EU level

Legislative change at EU level theoretically offers the greatest latitude for designing a minimum age policy as desired. Unlike the previous scenarios, one is not constrained by the pre-emptive effect of the DSA and other pre-existing EU legislation (although fundamental rights and international law, including the EU Treaty on the Functioning of the European Union (TFEU), must of course be respected). Naturally, *alignment and coherence* with existing legislation remain necessary and desirable.

A legislative amendment at EU level could, in theory, take the form of an amendment to the DSA, the AVMSD, the GDPR, or even a completely new Directive or Regulation. Completely new legislation, rather than an amendment, is in principle not conducive to the clarity and coherence of EU law, and also conflicts with the ambition of the Digital Omnibus initiative to simplify and streamline digital regulation in the EU. This option is therefore disregarded, and the focus below is on amendments.

An amendment or supplement to the DSA framework is the obvious choice, as this law has the most comprehensive and active enforcement framework. As explained in Chapter II.1, the European Commission has drawn up very detailed Guidelines on child protection, which also regulate the issue of age limits and age verification in detail. Several investigations are currently underway regarding age verification, including for pornography platforms and the social media platform Snapchat. Furthermore, national child protection legislation from other Member States ('the French model' discussed previously) has been designed for enforcement via the DSA. Placing this supervisory task with a different supervisory authority at this stage would therefore entail significant complications.

An amendment to the DSA could take many different forms in terms of its substance. The key substantive considerations were set out in Chapter IV.1. To summarise, the EU legislator could, for example, clarify or streamline the existing risk-based framework in certain respects (including by clarifying the European Commission's relevant powers or adjusting the burden of proof for age restrictions). Alternatively, categorical minimum age limits or verification requirements could be imposed for certain types of social media. These relatively minor changes to the existing framework would likely not justify a standalone legislative initiative, but could be incorporated into upcoming reforms such as the DFA.

Revisions related to the AVMSD appears less suitable for several reasons. Firstly, the relevant parts of the AVMSD focus on *video-sharing platforms*, whereas social media may, in principle, fall outside this definition. Secondly, the AVMSD has no supervisory authority at EU level, which could lead to further fragmentation of enforcement and result in a disproportionately large role being assigned to (among others) the Irish supervisory authority. Thirdly, this is a Directive rather than a Regulation, meaning that the harmonisation effect is weaker than under the DSA and implementation may vary between Member States and be subject to delays.

Any legislative reform at EU level would also present an opportunity to streamline the existing framework; as demonstrated in Chapter II.2, there is an unnecessary amount of substantive overlap between the child protection rules in Article 28b of the AVMSD and Article 28 of the DSA. Since the introduction of the DSA, the added value of Article 28b of the AVMSD has been limited, and consideration should be given to abolishing the overlapping obligations under this provision. To maintain an adequate level of protection, Article 28 of the DSA could potentially be expanded to compensate for the loss of safeguards under the AVMSD (for example, so that platforms continue to support the relevant AVMSD obligations of media service providers).[250] A comprehensive analysis of the possibilities goes beyond the scope of this report and warrants further elaboration in the ongoing review of the AVMSD.[251]

Ideally, the interaction between the DSA and the GDPR could also be clarified and streamlined. As discussed above, there is currently an ill-fitting division of competences, whereby the contractual minimum age falls under the DSA, and the rules on parental consent under the GDPR. An extension of the Commission's powers in this regard, or improved coordination mechanisms between supervisory authorities, could contribute to faster clarification and enforcement of the applicable rules.

250 In a 2025 report, the European Council concludes that Article 28b of the AVMSD still offers added value compared to the DSA. At the same time, it recommends that the Commission reassess this framework with a view to ensuring consistency with the DSA and possible simplification. A full analysis is beyond the scope of this current study. https://data.consilium.europa.eu/doc/document/ST-7710-2025-INIT/en/pdf.

251 https://digital-strategy.ec.europa.eu/en/news/commission-seeks-views-and-information-evaluation-audiovisual-media-services-directive.

4.3 Conclusions

Due to widespread public concern, there is now considerable pressure on public authorities to take an active role in protecting children on social media. However, this report has shown that there is no lack of relevant legislation. The ambitions set out in the coalition agreement are already reflected, to an appreciable extent, in the EU's current laws. Legislative amendments could refine or streamline this framework as regards certain details, but in our view, the main focus for achieving a minimum age for social media ought to be enforcement.

New legislative changes could impose an even higher minimum age. However, the potential changes compared to the current framework would be relatively limited. In practice, a lower age limit of 13 already applies, combined with parental consent requirements for those under 16. There are also good reasons for this tiered approach to age limits. Teenagers are given the opportunity to become acquainted with social media (in principle, via a safe version of the service), so that they can gain experience and develop resilience before they are granted unrestricted access at the age of sixteen. This tiered approach also ensures that platforms retain the incentive to continue investing in child protection measures. Where this framework currently falls short is in effective enforcement: the current minimum age and parental consent requirements are rarely, if ever, adhered to by major platforms and their users. There is also considerable room for improvement regarding platforms' implementation of other protective measures for young users (for example: limiting usage time).

A legislative amendment could also attempt to introduce stricter forms of age verification mandatory. Here too, however, the prospects are limited, not only because the current DSA framework already requires effective age verification, but also because even the strictest age verification obligations remain vulnerable to circumvention—for example, through the use of VPNs or with the help of adults. At the same time, there are significant risks to privacy and freedom of information. Our analysis therefore indicates that a further extension of the current framework to universal verification obligations for social media would be at odds with the fundamental rights of children and adults. The current DSA framework already imposes reasonable requirements regarding age verification, allowing the European Commission to monitor platforms' efforts on the basis of effectiveness and proportionality. As long as technical and societal conditions surrounding age verification remain in a state of flux, this flexible framework is advantageous, and the premature codification of stricter obligations remains risky.

The key opportunities for governments within this system may not lie in yet another legislative amendment to platform regulation, but rather in mobilising other societal actors. Parents can be encouraged to attend to overseeing their children's safe media use, through awareness campaigns highlighting the legal and contractual age limits already in place. Raising awareness of *parental controls* on laptops and smartphones could also be fruitful, including direct assistance in configuring these tools, for example by schools, libraries or other public institutions. At the same time, platforms must take appropriate measures under the DSA to ensure interoperability with these parental controls.

Although not of central importance, the following legislative changes could help to strengthen the current framework. At national level, the existing requirement for parental consent for those aged between 13 and 16, or, if desired, a binding minimum age of 15 or 16, could be codified into Dutch law. Such a legislative amendment at national level could help to communicate social norms and encourage voluntary compliance amongst young people, parents and third parties. Furthermore, this national standard could be enforced by the European Commission vis-à-vis platforms, via the DSA framework, so as to avoid any need for potentially complex and time-consuming coordination with GDPR supervisory authorities on this point. One possible problem with this approach is that the European Commission's current Guidelines appear to link such national minimum ages to strict verification obligations, which, in our view, may interfere (too) significantly with fundamental rights.

In the longer term, a legislative amendment at EU level, for example within the framework of the upcoming DFA, could aim to achieve the same: improved alignment between age standards for social media under the GDPR and the DSA, thereby facilitating swift and effective enforcement at European level. This could also be an opportunity to streamline unnecessary overlaps with the AVMSD. Alternatively, the existing powers of DSA supervisory authorities under Article 28 DSA could be further clarified and/or the burden of proof adapted (for example: explicit powers to prescribe minimum ages or verification obligations for unsafe social media; a codification of the industry-standard contractual minimum age of 13; or specifying other possible measures such as a curfew or time limits). In any case, we recommend that supervisory tasks relating to social media and child protection continue to be concentrated within the DSA framework, rather than being assigned to other authorities; ideally, this presents an opportunity to unify and strengthen supervisory tasks for child protection, rather than fragmenting them further.

5 References

American Psychological Association, 2023. Health Advisory on Social Media Use in Adolescence (APA Press). https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.

Baum, C. et al., 2024. Cryptographers' Feedback on the EU Digital Identity's ARF. https://www.cs.ru.nl/~jhh/publications/cryptographers-feedback.pdf.

Béjar, A. (2024, May 6). How to reduce the sexual solicitation of teens on Instagram. After Babel. https://www.afterbabel.com/p/make-social-media-safe-for-teens.

Bursztyn, L., et al, 2026. Why Bans Fail: Tipping Points and Australia's Social Media Ban. National Bureau of Economic Research Working Paper No. w35162. DOI: 10.3386/w35162

Castro, C. 2026. The EU's age verification app has a privacy problem — and it may be more than just a 'bug in an app'. TechRadar. https://www.techradar.com/vpn/vpn-privacy-security/the-eus-age-verification-app-has-a-privacy-problem-and-it-may-be-more-than-just-a-bug-in-an-app.

Eekelaar J. & Tobin J., 2019. 'Art. 3 the Best Interests of the Child' in: Tobin, J. (ed), The UN Convention on the Rights of the Child: A Commentary (Oxford: Oxford University Press 2019).

Galissaire, J. , 2025. Mind the Gap: Age Assurance and the Limits of Enforcement under EU Law. Interface. https://www.interface-eu.org/publications/age-assurance-gap.

Fornasier, M. (2015). The impact of EU fundamental rights on private relationships: direct or indirect effect?. European Review of Private Law, 23(1).

Helliwell, J. F. et al. (eds.), 2026. World Happiness Report 2026. University of Oxford: Wellbeing Research Centre.

Haidt, J., & Rausch, Z. (2025a, January 9). TikTok is harming children at an industrial scale. After Babel. https://www.afterbabel.com/p/industrial-scale-harm-tiktok.

Haidt, J., & Rausch, Z. (2025b, April 16). Snapchat is harming children at an industrial scale. After Babel. https://www.afterbabel.com/p/industrial-scale-snapchat.

Husovec, M., 2024. Principles of the Digital Services Act. Oxford University Press.

Jahangir, R. & Hendrix, J., 2026. Tracking Efforts To Restrict Or Ban Teens from Social Media Across the Globe. Tech Policy Press. https://www.techpolicy.press/tracking-efforts-to-restrict-or-ban-teens-from-social-media-across-the-globe/.

Koning, I. et al., 2025. Richtlijn Gezond Schermgebruik. Ministerie van Volksgezondheid, Welzijn en Sport. https://www.rijksoverheid.nl/documenten/rapporten/2025/06/17/richtlijn-gezond-schermgebruik-2025.

Lievens, E., 2021. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. Nordic Journal of Human Rights, 39(2), pp.128-145.

Livingstone, S. et al., 2024. Children's rights and online age assurance systems: The way forward. The International Journal of Children's Rights, 32(3), pp.721-747.

Lynskey, O., 2014. Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. International & Comparative Law Quarterly, 63(3), pp.569-597.

Martuzzi, M. & Tickner, J. (2004). The precautionary principle: protecting public health, the environment and the future of our children. World Health Organization.

Meerdere auteurs, 2026. Joint statement of security and privacy scientists and researchers on Age Assurance. https://csa-scientist-open-letter.org/ageverif-Feb2026.

Nair, A., 2018. The regulation of Internet pornography: Issues and challenges. Routledge.

National Academies of Sciences, Engineering, and Medicine, 2024. Social Media and Adolescent Health. (The National Academies Press).

Office of the Surgeon General, 2023. Social Media and Youth Mental Health: The US Surgeon General's Advisory. US Department of Health and Human Services. https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

Rieder, B. & Hofmann, J., 2020. Towards platform observability. Internet policy review, 9(4), pp.1-28.

Ritchie, H., 29 november 2024. Australia approves social media ban on under-16s. BBC News. https://www.bbc.com/news/articles/c89vjj0lxx9o.

Soares, J., 2026. The EU's Age Verification Fix May Create More Problems Than it Solves. Tech Policy Press. www.techpolicy.press/the-eus-age-verification-fix-creates-more-problems-than-it-solves/.

The Courier Mail, 7 maart 2026. 'Teens Still on Tiktok and Instagram Despite Ban', 7 maart 2026. https://www.couriermail.com.au/education/support/technology-digital-safety/teens-still-on-tiktok-instagram-despite-ban-as-experts-reveal-simple-workarounds/news-story/d7c3ad5343a791d7816caf8a88c8a179.

The Molly Rose Foundation, 2026. More than 60% of Australian children still using social media despite ban for under-16s, research shows. https://mollyrosefoundation.org/more-than-60-of-australian-children-still-using-social-media-despite-ban-for-under-16s-research-shows/.

UNESCO World Commission on the Ethics of Scientific Knowledge and Technology (2005). 'The Precautionary Principle'. https://unesdoc.unesco.org/ark:/48223/pf0000139578.

Van Dijck, J. & Jacobs, B., 2024. Electronic identity services as sociotechnical and political-economic constructs. New Media & Society 22(5). https://doi.org/10.1177/1461444819872537.

Van Gend, T. 2026. Europe's Age Verification Push Raises Privacy Issues Beyond Data Confidentiality. Tech Policy Press. https://www.techpolicy.press/europes-age-verification-push-raises-privacy-issues-beyond-data-confidentiality/.

Wilson, C. 2026. Most teens on social media pre-ban are still on those platforms, new data suggests. Crikey. https://www.crikey.com.au/2026/03/13/teens-social-media-ban-kids-still-using-platforms/.

IViR - Institute for Information Law
P.O. Box 15514, 1001 NA Amsterdam, the Netherlands

https://www.ivir.nl/