Universiteit
Leiden
The Netherlands

Behavioural profiling for age assurance: do the ends justify the means?

Shaffique, M.R.; Hof, S. van der

Citation
Shaffique, M. R., & Hof, S. van der. (2025). Behavioural profiling for age assurance: do the ends justify the means? *International Data Privacy Law*, *16*(1), 1-17. doi:10.1093/idpl/ipaf012

Version:	Publisher's Version
License:	Creative Commons CC BY 4.0 license
Downloaded from:	https://hdl.handle.net/1887/4292118

Note: To cite this publication please use the final published version (if applicable).

Behavioural profiling for age assurance: do the ends justify the means?

Mohammed Raiz Shaffique * and Simone van der Hof †

Key Points

- Age assurance is an increasingly relevant topic from a socio-legal perspective and behavioural profiling, that is, determining the age of users by profiling their online behaviour, is one method of age assurance.
- While behavioural profiling for age assurance might be a relatively frictionless method of implementing age assurance, it poses concerns from a privacy, accuracy, and non-discrimination standpoint.
- Legislation, including the General Data Protection Regulation, the Digital Services Act, the Audio Visual Media Services Directive, and the Artificial Intelligence Act, apply in different manners to behavioural profiling for age assurance, and there are legitimate grounds to conclude that behavioural profiling should be subjected to strict scrutiny and may not be a proportionate and thus lawful form of age assurance.
- Despite several concerns regarding behavioural profiling for age assurance, digital service providers such as TikTok, Meta, and Google employ this practice, possibly leveraging existing commercial profiling mechanisms for this purpose.
- Even if behavioural profiling is convenient for digital service providers owing to reduced user friction, this cannot be a justification for employing such age assurance methods instead of privacy-friendly and effective age verification techniques, particularly when age verification is legally mandated.

Introduction

The fact that today we are living in an online environment where digital service providers extensively mine, collect, and use the data of users and build their profiles for commercial, and at times even political purposes, is an extensively written about topic.[1] However, profiling of users need not always be for commercial or political purposes, and may also be for ascertaining the age of an online user, and this is where age assurance comes in. Age assurance, that is, the various methods used for finding the age of online users, has emerged as a contemporary topic of socio-legal relevance.[2] Various stakeholders view age assurance as a tool to protect children online, including by preventing them from accessing harmful content and services. Behavioural profiling is one such method of age assurance whereby algorithmic analysis is employed to study the online activities of users and estimate their age.[3] While age assurance in general is legally relevant in different ways as per European Union (EU) law,[4] whether behavioural profiling is a legally acceptable form of age assurance is less clear. On the one hand,

* Mohammed Raiz Shaffique, PhD Candidate, eLaw-Center for Law and Digital Technologies, University of Leiden, Leiden, The Netherlands. Email: m.r.shaffique@law.leidenuniv.nl.

† Simone van der Hof, Professor, eLaw-Center for Law and Digital Technologies, University of Leiden, Leiden, The Netherlands. Email: s.van.der.hof@law.leidenuniv.nl.

1 eg Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019); A Zardiashvili, 'Power and Dignity: The Ends of Online Behavioral Advertising in the European Union' (PhD thesis, Leiden University 2024) <https://hdl.handle.net/1887/3753619> accessed 30 September 2024.

2 Mohammed Raiz Shaffique and Simone van der Hof, 'Research Report: Mapping Age Assurance Typologies and Requirements' (*European Commission*, February 2024) 10, 12 <https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements> accessed 29 July 2024.

3 Information Commissioner's Office, 'Age assurance for the Children's code' (January 2024) 9 <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/> accessed 29 July 2024.

4 For an elaboration of the different ways in which age assurance is legally relevant, see Shaffique and van der Hof (n 2) 15–24.

© The Author(s) 2025. Published by Oxford University Press.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

behavioural profiling as a method of age assurance has certain benefits over other age assurance methods, while on the other hand, behavioural profiling also poses several risks to the rights of online users, including children. What makes behavioural profiling particularly pressing to address is the fact that it can provide an avenue for digital service providers to legitimize the profiling of users, including children, which can have detrimental impacts on the rights and freedoms of online users. It can be seen from the publicly available information that at least three of the larger online platforms, ie Meta,[5] TikTok,[6] and Google,[7] employ behavioural profiling for age assurance, meaning that millions of users are being subjected to this practice.

Therefore, the present article delves into a deeper analysis of behavioural profiling as a method of age assurance, including an examination of the socio-legal implications of the same. To this end, the following section 'Behavioural profiling as a method of age assurance' provides an outline of what age assurance is and how behavioural profiling relates to age assurance. That section also analyses the advantages and disadvantages of behavioural profiling. Thereafter, the section 'Legal analysis of behavioural profiling for age assurance under the GDPR, DSA, AVMSD and AI Act' elucidates how various EU statutes, specifically the General Data Protection Regulation[8] ('GDPR'), the Digital Services Act[9] ('DSA'), the Audio Visual Media Services Directive[10] ('AVMSD') and the Artificial Intelligence Act[11] ('AI Act'), legally govern behavioural profiling for age assurance. The final section is the conclusion of the article. It is pertinent to mention that the present article focuses on situations where digital service providers profile users to estimate their age, regardless of whether that profiling is solely for age assurance purposes or is part of a broader profiling strategy, including for commercial purposes.

Behavioural profiling as a method of age assurance

The legal relevance of age assurance

Recent times have seen an increasing focus on the topic of age assurance by policymakers, regulators, civil society organizations, and industry. This is primarily from the perspective of how age assurance can be used to further the safety of children online. Although navigating safe digital environments contributes to children's rights, age assurance itself should also not violate children's rights (eg the right to be heard).[12] The European Commission, in its Better Internet for Kids+ strategy, states that it will draft a request for a European standard on age verification online, so as to safeguard children from online risks and promote their rights and well-being.[13] The European Commission also has a task force to identify the best practices for age verification,[14] and released a research report concerning age assurance that explains when age assurance is or may be legally required and what types of and requirements for age

5 Pavni Diwanji, 'How Do We Know Someone Is Old Enough to Use Our Apps?' (*Meta*, 27 July 2021) <https://about.fb.com/news/2021/07/age-verification/> accessed 30 July 2024.

6 Sarah Perez, 'TikTok CEO says Company Scans Public Videos to Determine Users' Ages' (*TechCrunch*, 23 March 2023) <https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEHI9shXsCY5yADl8eEggLmgAa8-6ij9iYFiEjyAyMOl2jHxr3NQbEIjGUDwQmPid_36MZUp0wfuiY7rBJVgL1AxKMm_xyQPFqAxEujtMh9qXIyPiJC23OcdjbINbmm4pNXJo-2nApiIpAPLysF_3aD8ZsIsea_iHNn4Rw4sxeeo> accessed 30 July 2024; TikTok, 'Privacy Policy' (19 November 2023) <https://www.tiktok.com/legal/page/eea/privacy-policy/en> accessed 30 July 2024.

7 Google, 'Privacy & Terms' <https://policies.google.com/privacy?hl=en-US#whycollect> accessed 30 July 2024.

8 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

9 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) [2022] OJ L277/1.

10 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018], OJ L303/69, art 28b(3)(f).

11 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L2024/1689.

12 Sonia Livingstone and others, 'Children's Rights and Online Age Assurance Systems: The Way Forward' (2024) 32 International Journal of Children's Rights 721 <https://brill.com/view/journals/chil/32/3/article-p721_009.xml> accessed 28 October 2024.

13 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+)' (Communication) COM(2022) 212 final.

14 European Commission, 'Digital Services Act: Task Force on Age Verification' (Shaping Europe's Digital Future, 30 January 2024) <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0> accessed 28 October 2024; European Commission, 'Second Meeting of the Task Force on Age Verification' (Shaping Europe's Digital Future, 20 March 2024) <https://digital-strategy.ec.europa.eu/en/news/second-meeting-task-force-age-verification> accessed 1 August 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

assurance exist.[15] Moreover, age assurance as a measure to protect children online is—depending on the context and risks involved—required or suggested to be used by video platforms and online platforms respectively in the AVMSD and the DSA.

From an EU perspective, there are different ways in which age assurance can be seen as legally relevant:

(i) Laws that require persons to be of a given minimum age to access certain products and services (eg gambling activities) or to execute certain legal acts (eg entering into contracts) mandate age assurance for legal compliance. For instance, Article 6a and Article 28b AVMSD require that audiovisual media service providers and video-sharing platforms protect children from harmful content. When it comes to most harmful content (gratuitous violence, pornography, etc), strict measures such as effective age verification systems can be required;

(ii) Laws that impose a duty of care on digital service providers to protect children may consider age assurance as an appropriate measure. For example Article 28 DSA places a duty on online platforms to implement measures to provide a high level of privacy, safety, and security to children. To fulfil this duty of care, age assurance may be an apt measure, though it is not mandated as the recommended measure in the provision; and

(iii) Contractual obligations requiring the products or services to be made available to only users of certain ages may require age assurance for contractual compliance. For example a third party might bind the online platform to a contractual clause that the latter's services be provided only to users above a certain age. As compared to (i) and (ii) above, this stipulation is not externally imposed by public law but can still be enforceable through contract law.[16]

It is also possible that platforms may wish to implement age assurance in the absence of legal or contractual obligations, because the digital service provider considers it as an appropriate measure owing to the risks faced by children using the service.[17]

In other countries too, attention for age assurance is growing, and legal requirements are emerging that may oblige digital service providers to implement age assurance. In the UK, the Online Safety Act 2023 mandates certain digital service providers to implement age assurance to protect children online.[18] The statute also tasks the Office of Communications (Ofcom) with providing guidance on, and monitoring compliance with, such age assurance obligations.[19] In the USA, several legislations at the State level require age verification to be implemented by platforms that host content that is considered harmful to minors.[20] The underlying reasoning behind such initiatives is that measures which can prevent children from accessing age-inappropriate services and which can prevent adults from accessing child-friendly spaces could help in combating the risks faced by children in the online sphere.[21] In fact, in December 2024, Australia amended the Online Safety Act, 2021,[22] to require social media platforms to take 'reasonable steps' to restrict children who are below 16 years.[23] This requirement takes effect in December 2025, and while there are no specifics yet on the age assurance methods that will be considered acceptable, the eSafety Commissioner is slated to play a leading role in implementing this online age restriction.[24]

Several civil society organizations,[25] industry bodies[26] and standardization entities[27] have published

15 Shaffique and van der Hof (n 2).

16 For an elaboration of the different ways in which age assurance is legally relevant, see Shaffique and van der Hof (n 2) 15–24.

17 ibid 24.

18 Online Safety Act 2023, ss 12 and 81.

19 Online Safety Act 2023, ss 82, 157, 161, and 164.

20 Congressional Research Service, 'Identifying Minors Online' (2 January 2024) 2 <https://crsreports.congress.gov/product/pdf/R/R47884/6> accessed 29 July 2024.

21 The different types of risks faced by children online has been classified by the Organisation for Economic Co-operation and Development. See Organisation for Economic Co-operation and Development, 'Children in the digital environment: Revised typology of risks' (2021) <https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en> accessed 1 August 2024.

22 Online Safety Act 2021 (Australia).

23 Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australia), cls 1 and 2.

24 eSafety Commissioner, 'Social media age restrictions' <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions> accessed 9 March 2025.

25 eg 5 Rights Foundation, 'But How Do they Know it is a Child? Age Assurance in the Digital World' (October 2021) <https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf> accessed 29 July 2024; UNICEF, 'Digital Age Assurance Tools and Children's Rights Online across the Globe: A Discussion Paper' (April 2021) <https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf> accessed 29 July 2024.

26 eg Digital Trust and Safety Partnership, 'Age Assurance: Guiding Principles and Best Practices' (September 2023) <https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf> accessed 1 August 2024.

27 eg IEEE, 'IEEE Approved Draft Standard for Online Age Verification' (February 2024); ISO, 'ISO/IEC WD 27566-1. Information security, cybersecurity and privacy protection. Age assurance systems Framework. Part 1: Framework' <https://www.iso.org/standard/88143.html> accessed 1 August 2024; ISO, 'ISO/IEC WD 27566-2: Age assurance systems. Part 2: Benchmarks for benchmarking analysis' <https://www.iso.org/standard/88147.html> accessed 1 August 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

various works dealing with the diverse aspects pertaining to age assurance. Regulators in the sphere of data protection and content regulation across Europe have taken heed of the importance of age assurance in today's times.[28] The diverging discussions surrounding age assurance show that it is a complex topic which cannot be seen as a panacea for online child protection, and the implementation of age assurance very much depends on the facts and circumstances surrounding particular online platforms and their users.[29]

Accordingly, since the socio-legal contemporary relevance of age assurance is clear from the above, it would be appropriate to delve into the topic of this article—behavioural profiling, a method of age assurance used by online platforms.

Behavioural profiling as age assurance

Age assurance is used as an umbrella term for the various techniques employed to ascertain an individual's age or age range.[30] There are three categories of age assurance, that is (i) age estimation, (ii) age verification, and (iii) self-declaration.[31] The present article deals specifically with age estimation, which essentially relates to those types of age assurance where the possible age of a user is assessed using methods such as estimation based on facial analysis and online behavioural analysis.[32] Contrary to age verification, where the endeavour is to determine the exact age or age range of a user, age estimation results in assessing an approximate age or age range.[33] Age estimation can be employed at the time of initially allowing an individual to use the platform or for monitoring while they are using the platform.[34] There are several methods of age estimation present today, and behavioural profiling is one of the methods, with other such methods being facial age estimation,[35] capacity testing,[36] and so on.[37] Below, Figure 1 shows the relation between behavioural profiling and age assurance.

Generally, profiling in the online sphere is the mechanism by which data is processed by platforms to infer information about users or their behaviour.[38] The GDPR defines profiling as a method of 'automated processing of personal data' to analyse or predict attributes of a person, such as their financial or health situation, or their interests or behaviour.[39] Though evaluation or prediction of a person's age through profiling is not specifically mentioned in this definition, the expansive wording of Article 4(4) GDPR means that age-related analysis would also amount to profiling. The scope of profiling under GDPR is wide and does not require detailed personality profiles to be developed, and often 'the evaluation of singular and sometimes (seemingly) unimportant personal aspects is covered by the definition'.[40]

When users' online activities are analysed using artificial intelligence (AI) to estimate their age in particular, this method of age estimation is called behavioural profiling.[41] The nature of such algorithmic analysis may be multi-fold and can involve analysing a person's digital activities across platforms.[42] To this end, various data points may be analysed that reflect online behaviour, including content and activities liked and shared, a person's social connections, public posts, private chats, browsing and purchase history, mouse, and keyboard use, etc.[43]

Thus, behavioural profiling is essentially a way of inferring a person's age attributes using an AI model that studies patterns and makes predictions.[44] There are also third-party service providers offering such behavioural analytics services to estimate age using technology that can 'monitor key strokes, typing speed, time of day the

28 Ofcom, 'Guidance on highly effective age assurance For Part 3 services' (16 January 2025) <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=388809> accessed 9 March 2025; Agencia Española de Protección de Datos, 'Decálogo de principios. Verificación de edad y protección de personas menores de edad ante contenidos inadecuados' (December 2023) <https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf> accessed 30 July 2024.

29 Shaffique and van der Hof (n 2).

30 ibid 12.

31 euCONSENT, 'D5.1 Common Vocabulary' (29 June 2021) 4 <https://euCONSENT.eu/project-deliverables/> accessed 29 July 2024.

32 'CEN and CENELEC, Age appropriate digital services framework' (September 2023) 10 <https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf> accessed 29 July 2024; Shaffique and van der Hof (n 2) 12.

33 Shaffique and van der Hof (n 2) 13.

34 Information Commissioner's Office (n 3) 9.

35 Facial age estimation is where facial analysis of users is performed with AI to estimate their age. See *euCONSENT*, 'D2.2 EU Methods for AVMSD and GDPR Compliance Report' (2 January 2022) 10 <https://euCONSENT.eu/project-deliverables/> accessed 29 July 2024.

36 Capacity testing is where age of the users is estimated by testing aptitude or capacity, ie by making them do language tests, puzzles etc See 5Rights Foundation (n 25) 33.

37 Martin Sas and Jan Tobias Mühlberg, 'Trustworthy Age Assurance?' (*The Greens EFA*, February 2024) 50–57 <https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance> accessed 29 July 2024.

38 5Rights Foundation (n 25) 31.

39 GDPR, art 4(4).

40 Klaus Wiedemann, 'Profiling and (Automated) Decision-making under the GDPR: A Two-step Approach' (2022) 45 Computer Law & Security Review 3 <https://doi.org/10.1016/j.clsr.2022.105662> accessed 29 July 2024.

41 Shaffique and van der Hof (n 2) 13.

42 Information Commissioner's Office (n 3) 9.

43 Tony Allen and others, 'Measurement of Age Assurance Technologies' (*Age Check Certification Scheme*, 2022) 21–22 <https://ico.org.uk/media/about-the-ico/documents/4021822/measurement-of-age-assurance-technologies.pdf> accessed 29 July 2024.

44 Information Commissioner's Office (n 3) 9.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

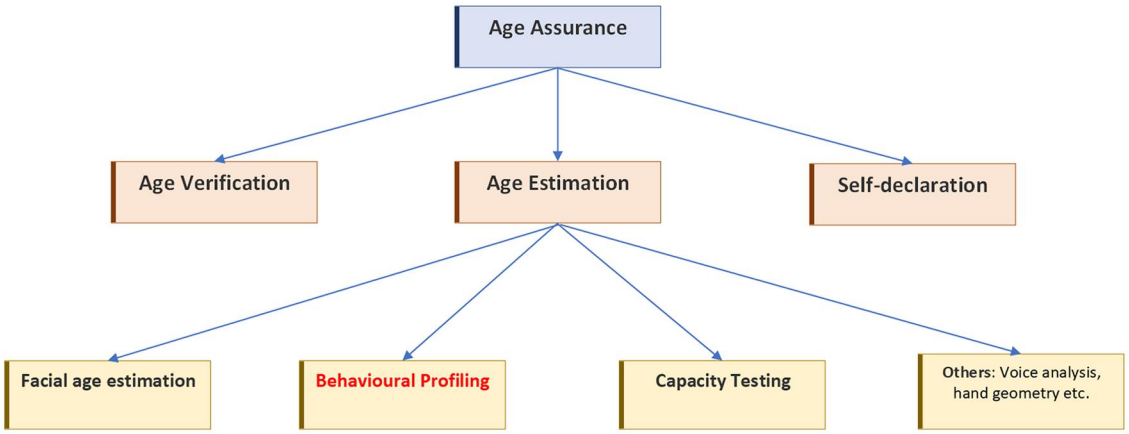

Figure 1. Relation between age assurance and behavioural profiling

user logs on, and other granular data'.[45] The accuracy of such age estimations depends on the AI technology employed and the reliability of the dataset used to train the AI system.[46]

There is little by way of public disclosure by digital service providers regarding the deployment of such AI systems and their accuracy.[47] In 2021, *Meta* stated that it had developed AI-based technology to estimate users' age by looking at online user behaviour, with the stated objective of differentiating between child and adult users.[48] Meta's AI model, which is termed 'adult classifier', is trained using data that includes profile information of a user and how the user interacts with other users and content.[49] Online user activity, such as what age is revealed from the birthday greetings received by the user and whether there is any discrepancy in the ages disclosed in different platforms, such as Facebook and Instagram, is analysed by the AI to this end.[50] Meta collects a whole range of data from its users' activity, as mentioned in Meta's privacy policy.[51] However, Meta does not expressly state in its privacy policy that such data is used for ascertaining the age of users, though such a measure can possibly fall under the more generic objective stated by Meta of promoting 'safety, security and integrity' by verifying user accounts. There is also no publicly available data on the number of users subjected to such behavioural profiling and the accuracy of the same.

Although behavioural profiling is used as a method of age assurance, it is not mandated in laws or standards as a method of age assurance to be implemented. Moreover, in situations where age *verification* is legally required, behavioural profiling, being a form of age *estimation*, would not be a sufficient measure to fulfil such legal requirements.

The relation between behavioural profiling as age estimation and commercial profiling

Behavioural profiling can be performed for different purposes that may be interrelated. As explained in the previous section, profiling may be deployed by a platform with the main purpose of estimating the age of the users to remove or restrict users below the minimum age criteria. However, profiling activities may also be carried out by a digital service provider for other, often for commercial and marketing, purposes, and these profiles may provide an estimate of the user's age, which can then be used for age assurance purposes.

In the era of 'surveillance capitalism', in which the economic model of digital service providers revolves

45 UNICEF (n 25) 29.

46 eSafety Commissioner, 'Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography' (August 2023) 153 <https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf> accessed 29 July 2024.

47 In, eg a decision by the Irish Data Protection Commission in the matter of TikTok Technology Limited references to age verification technologies used by TikTok have been blacked out; *In the matter of TikTok Technology Limited* Data Protection Commission Inquiry Reference: IN-21-9-1 [2023] <https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf> accessed 30 July 2024.

48 Diwanji (n 5).

49 Erica Finkle and others, 'How Meta uses AI to Better Understand People's Ages on our Platforms' (*Meta*, 23 June 2022) <https://tech.facebook.com/artificial-intelligence/2022/6/adult-classifier/> accessed 30 July 2024.

50 Diwanji (n 5).

51 Instagram, 'Data Policy | Instagram Help Centre' <https://help.instagram.com/155833707900388?cms_id=155833707900388> accessed 8 October 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

around monitoring user behaviour, collating user data, and targeting users with personalized (and often manipulative) content and interactions,[52] it is inevitable that platforms find it profitable to increasingly profile users. Data points emanating from any and all user activity are processed through 'advanced predictive tools with large data sets' to predict user behaviour.[53] In effect, this has led several large companies to develop and share digital profiles of users, which can reveal a wide range of predictions about the users, including their interests and age range.[54] The primary objective behind such commercial profiling is to provide targeted advertisements and enhance user engagement.[55] Both parents and children have seen this interconnection between behavioural profiling and commercial profiling as an important factor to be apprehensive of behavioural profiling.[56] They feel that the profiling activities that already occur online is overwhelming, and thus, employing profiling for age assurance is also not preferable.[57]

The authors' investigation has revealed that at least three of the larger platforms, being TikTok,[58] Meta,[59] and Google,[60] perform behavioural profiling for age assurance. It is unclear whether this is part of a larger commercial profiling framework of these platforms. However, given the widespread commercial profiling practices present today, it is possible or even plausible that behavioural profiling as age estimation is part of ongoing commercial profiling of users on digital platforms, rather than behavioural profiling being done specifically for just age estimation. This is relevant given that commercial profiling of children is more strictly regulated.[61] This raises the question of what that means if behavioural profiling is done partly for age estimation, a purpose that, unlike profiling for commercial purposes, may be in the best interests of children. Moreover, the law may expressly provide that data of children processed for the purpose of their online protection, such as for age assurance, may not also be used for commercial purposes, such as profiling.[62] That raises the question of what that means for commercial profiling, based on which age estimation is performed. The objective of this article is to legally analyse behavioural profiling as age estimation, both when the main or sole purpose is age estimation and also when it is done as part of a broader process of (commercial) profiling users.

Advantages and disadvantages of behavioural profiling as age estimation

Behavioural profiling as age estimation has both positive and negative aspects. There are certain advantages to using behavioural profiling as age assurance as compared to other methods.[63] First, it can prevent the exclusion of children who do not have official documents from the online platforms.[64] For instance, if platforms require children to prove their age using identification documents,[65] this can negatively affect children who do not have such documents (perhaps due to socio-economic reasons). Secondly, the Information Commissioner's Office (ICO) in UK states that behavioural profiling may be more privacy-friendly than using official documents for age assurance,[66] ostensibly as the data relating to such documents need not be processed. However, behavioural profiling is unlikely to have such an advantage from a privacy perspective in most situations, as elaborated below. Thirdly, this method can be a useful tool in identifying those children below the minimum age requirement, through ongoing monitoring, when the children have somehow circumvented initial age assurance measures.[67] For example, if the age assurance method employed by the platform is that of requiring identification documents or credit card details at the time of signing up, children may circumvent this using the documents of an adult. Fourthly, behavioural profiling does not hinder functionality for users while using a platform, as compared to other methods where the age assurance process requires users to complete certain steps before entering the platform, thereby resulting in user friction.[68] This

52 Zuboff (n 1).

53 Jane Andrew and Max Baker, 'The General Data Protection Regulation in the Age of Surveillance Capitalism' (2021) 168 Journal of Business Ethics 565, 566.

54 UNICEF (n 25) 28.

55 5Rights Foundation (n 25) 31–32; On behavioural advertising see Zardiashvili (n 1).

56 Revealing Reality, 'Families Attitude towards Age Assurance' 23 <https://www.drcf.org.uk/__data/assets/pdf_file/0037/258688/Families-attitudes-towards-age-assurance.pdf> accessed 30 July 2024.

57 ibid.

58 Perez (n 6); TikTok, Privacy Policy (n 6).

59 Diwanji (n 5).

60 Google, 'Privacy & Terms' (n 7).

61 Simone van der Hof, Eva Lievens and Ingrida Milkaite, 'The GDPR and Children's Personal Data' (*The Oxford Encylopedia of EU Law*, OUP 2022).

62 See, eg AVMSD, art 28b(3). See also DSA, art 28(3).

63 See for an overview of potential methods: Shaffique and van der Hof (n 2) 25–36.

64 UNICEF (n 25) 27–28.

65 Known as the 'Hard identifiers' method of age assurance, this is when verified identity documents (eg passports and driving licenses) are used to ascertain the age of a user. See Shaffique and van der Hof (n 2) 26–27.

66 Information Commissioner's Office (n 3) 9.

67 eSafety Commissioner (n 46) 154.

68 5Rights Foundation (n 25) 32.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

can be an attractive element from the perspective of companies, since it avoids the possibility of users migrating to alternate platforms where they may find the age assurance process less cumbersome.

However, behavioural profiling also poses certain risks which can be broadly placed into three categories, that is (i) Privacy, (ii) Accuracy, and (iii) Non-discrimination.

(i) Privacy—Behavioural profiling may have an uneasy relationship with children's rights, especially because of the privacy-invasive manner in which children's online behaviour is analysed to make age predictions.[69] As mentioned earlier, the method may involve analysing different kinds of user data, ranging from public content shared on platforms to private chats with birthday wishes.[70] This can result in an erosion of a user's right to privacy and data protection, which is a fundamental right under Articles 7–8 Charter of Fundamental Rights of the EU[71] ('Charter').[72] There is also the added concern of such profiling data being shared with third parties or used for commercial or political purposes[73] (eg for targeted advertisements or for influencing voters based on their political beliefs). Notably, for behavioural profiling to be effective in estimating users' age, platforms would have to monitor the behaviour of all users and not just child users, thus posing a privacy risk to all users, irrespective of whether they are children.

Moreover, digital service providers and third parties providing behavioural age analytics may be motivated to process larger amounts of users' (including children's) data to improve the accuracy of their systems, posing a further challenge to online privacy.[74] This may in fact incentivize data collection and profiling of users even more than is already the case.[75] There is also the possibility that behavioural profiling may provide a surreptitious legitimacy to such privacy-invasive measures, as platforms may claim that their profiling activities are for user well-being. It could be practically difficult to ascertain the contours of commercial profiling and behavioural profiling, and to ensure that the latter is not used as a means to complement the former. One study found that children and their parents rarely looked favourably on behavioural profiling, due to the privacy-invasive manner of the measure.[76] Such reservations are exacerbated when private messages and content, as opposed to public posts, are analysed for profiling purposes.[77] There is also rarely transparency on how such systems are used and how age-related decisions are arrived at, further increasing privacy concerns. In this regard, in congressional hearings in the USA, *TikTok*'s Chief Executive Officer indicated that the platform uses tools that evaluate the public profiles of the users, including videos uploaded by them, to determine whether the age of the user in the video confirms with age declared by the user.[78] TikTok's policy concerning users challenging the platform's decision to restrict their usage due to being underage states that TikTok may ban users or restrict functionalities for users if the platform 'believe[s]' that the minimum age requirements are not met.[79] Therefore, it is possible that one of the ways in which the platform gains such 'belief' that an existing user is not of sufficient age is by perusing the user's online behaviour and estimating their age based on the same. TikTok's privacy policy does state that the information shared by users is used to enforce its terms and policies and that the users' content is reviewed through automated means for furthering safety.[80] Though the European Data Protection Board (EDPB) looked into the age verification practices of TikTok as part of the Irish Data Protection Commission's proceedings, the particulars of the actual practices employed were not made publicly available in the EDPB decision.[81]

(ii) Accuracy—When age assurance is implemented, accuracy is an indispensable requirement, as otherwise the objective of online child safety will not be met.[82] Being an AI-based system, the accuracy

69 UNICEF (n 25) 29–30.

70 Allen (n 43) 21–22.

71 Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.

72 Children have a right to privacy under UN CRC, art 16. This right has been interpreted by the UN Child Rights Committee to also include a right to data protection: see Committee on the Rights of the Child, 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment' (2 March 2021) 11–13 <https://digitallibrary.un.org/record/3906061> accessed 28 October 2024.

73 5Rights Foundation (n 25) 32; Sas and Mühlberg (n 37) 51.

74 Scott Babwah and Brennena Matt Perault, 'Keeping Kids Safe Online: How Should Policymakers Approach Age Verification?' (*Center for Growth and Opportunity*, June 2023) 5 <https://www.thecgo.org/wp-content/uploads/2023/06/Age-Assurance_03.pdf> accessed 29 July 2024; Congressional Research Service (n 20) 8.

75 European Digital Rights, 'Online Age Verification and Children's Rights' (4 October 2023) 22 <https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf> accessed 29 July 2024.

76 Revealing Reality (n 56) 23.

77 ibid 23–24.

78 Perez (n 6).

79 TikTok, 'Minimum Age Appeals on TikTok' <https://support.tiktok.com/en/safety-hc/account-and-user-safety/minimum-age-appeals-on-tiktok> accessed 30 July 2024; TikTok, 'Underage Appeals on TikTok' <https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok> accessed 30 July 2024.

80 TikTok, Privacy Policy (n 6).

81 In the matter of TikTok Technology Limited (n 47).

82 Shaffique and van der Hof (n 2) 42.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

inevitably depends on the quality of the dataset that is used to train the AI to make age-related predictions based on online behaviour.[83] Though it is possible for such algorithmic analysis to be accurate, this is far from a given[84] due to the inherent vulnerabilities of AI systems in general.[85] The potential for inaccuracy is also high, as online behaviour may not be indicative of the age of a user.[86] Studies on the accuracy of estimating the age of users based on their social media activities and mobile phone usage do not provide conclusive evidence on the reliability of such methods beyond a reasonable doubt.[87] Especially when the quality of training data is not adequate, the level of assurance provided by behavioural profiling can be low.[88] Moreover, the accuracy of such an analysis of online behaviour may also be hampered when user accounts and devices are shared by multiple people, as often happens with children and their friends and family.[89] Such lack of accuracy may result in users being wrongly denied access to platforms and children being given access to inappropriate (functionalities of) services and content.[90]

(iii) Non-discrimination—A concern closely related to accuracy is that the inaccurate age assurance decisions based on behavioural profiling may itself lead to discrimination.[91] Age-based categorization of users, relying on presumed behavioural norms, assumes that a person's online behaviour reflects their biological age.[92] This can discriminate against those who do not fit these archetypes and are not considered old enough to use a platform, thus denying them access to services. Such a risk becomes even greater for people with disabilities or neurodiversity.[93] There is also the aspect that such behaviour-based online age determinations are not sensitive to cultural contexts and how they differ globally,[94] which again can raise the possibility that users from certain cultures may be discriminated against by algorithmic decisions. This can result in behavioural profiling methods violating the right to non-discrimination in Article 21 Charter and Article 2 United Nations Convention on the Rights of the Child ('UN CRC').

Interim conclusion

Due to the above concerns, behavioural profiling has been said to be contrary to the best interests of the child[95] and a disproportionate method of age assurance.[96] However, some regulators have stated that behavioural profiling is not prohibited as an age assurance measure and may even be appropriate in certain circumstances. The ICO has indicated that behavioural profiling is an acceptable method of age assurance method provided that it is implemented in a proportionate manner, that there is sufficient confidence in the accuracy and fairness of the process and that the data used for profiling is not used for other purposes.[97] The ICO also seems to convey that the information collected by such behavioural profiling methods could also be used to determine the number of children using a particular platform.[98] The eSafety Commissioner in Australia has also suggested that behavioural profiling may be appropriate as a second level of age assurance process at some platforms, based on the level of risk involved and provided that transparency and purpose limitation norms are met.[99] It is stated that behavioural profiling can be an important secondary tool on certain platforms, to complement the self-declaration method or to identify 'children who have bypassed age assurance measures used at the sign up stage'.[100]

However, given the serious problems users may face as a result of behavioural profiling, it is difficult to accept such tacit regulatory approval at face value. The

83 eSafety Commissioner (n 46) 153; Sas and Mühlberg (n 37) 51.
84 UNICEF (n 25) 28.
85 Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans* (Pelican Books 2020), Ch 6.
86 Sas and Mühlberg (n 37) 51.
87 eSafety Commissioner (n 46) 154.
88 5Rights Foundation (n 25) 32.
89 UNICEF (n 25) 29.
90 Shaffique and van der Hof (n 2) 32.
91 UNICEF (n 25) 30.
92 Shaffique and van der Hof (n 2) 32.
93 Sas and Mühlberg (n 37) 52.
94 UNICEF (n 25) 29; European Digital Rights (n 75) 22.
95 Simone van der Hof and Sanne Ouburg, 'D2.3 Methods for Obtaining Parental Consent and Maintaining Children Rights' (*euCONSENT*, 25 June 2021) 24 <https://hdl.handle.net/1887/3494449> accessed 29 July 2024; Simone van der Hof and Sanne Ouburg, '"We Take Your Word for It"-A Review of Methods of Age Verification and Parental Consent in Digital Services' (2022) European Data Protection Law Review 8, 65 <https://edpl.lexxion.eu/article/EDPL/2022/1/10> accessed 30 July 2024.
96 Sas and Mühlberg (n 37) 52.
97 Information Commissioner's Office (n 3) 30.
98 Information Commissioner's Office, '"Likely to be accessed" by Children—FAQs, List of Factors and Case Studies.' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/#threshold> accessed 29 July 2024.
99 eSafety Commissioner (n 46) 154.
100 ibid.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

Spanish Data Protection Authority has even stated that user profiling is not necessary for age assurance.[101] Notably, Ofcom's guidance on age assurance does not mention behavioural profiling as either an effective or an ineffective method.[102] In Ofcom's statement on age assurance and children's access, the contrasting positions of different stakeholders on behavioural profiling were recorded, but no view was expressed by Ofcom.[103] However, Ofcom clarified that it does not recommend behavioural profiling of users as a method for platforms to ascertain if a large number of their users are children.[104] It would therefore be relevant to look at how the EU legal regime deals with behavioural profiling, in order to assess whether there is sufficient legal justification for using it as a method of age assurance. To this end, the next section analyses how behavioural profiling is regulated by the GDPR, the DSA, the AVMSD, and the AI Act.

Legal analysis of behavioural profiling for age assurance under the GDPR, DSA, AVMSD, and AI Act

To determine whether behavioural profiling for age assurance is a proportionate tool, a legal analysis of age assurance should be carried out. Age assurance may be necessary to comply with the law (see the subsection 'The legal relevance of age assurance'), but age assurance itself must also comply with the law. For instance, according to the EDPB, age assurance is likely to pose a high risk to the rights and freedoms of data subjects in many cases, thus necessitating a Data Protection Impact Assessment as per Article 35 GDPR.[105] Thus, most prominent is the use of data in behavioural profiling for age assurance and therefore the question of whether and how this form of age assurance complies with the GDPR, particularly in view of the higher level of data protection for children (see the subsection 'Behavioural profiling as age assurance under the GDPR'). Moreover, while the DSA provides that age assurance is a possible mitigating measure to protect children's privacy, safety, and security online and more specifically safeguard them against certain risks in the design of (very large) online platforms, it is also stated that age assurance should respect user privacy (see the subsection 'Behavioural profiling as age assurance under the DSA'). The AVMSD recognizes age verification as a relevant measure to prevent children from accessing age-inappropriate content, while specifying that personal data of minors used for such measures should not be used for behaviour-based advertising (see the subsection 'Behavioural profiling as age assurance under the AVMSD'). Finally, behavioural profiling for age assurance uses AI, making it important to analyse to what extent the AI Act has an impact on this method of age assurance (see the subsection 'Behavioural profiling as age assurance under the AI Act'). Where relevant, the interplay between these regulations is also explained in relation to behavioural profiling as age assurance.

Behavioural profiling as age assurance under the GDPR

To create a behavioural profile, personal data must be processed from individuals, and the GDPR therefore applies to this processing activity. Moreover, behavioural profiling is covered by the definition of profiling in the GDPR (see the subsection 'Behavioural profiling as age assurance'). Profiling of individuals enjoys particular attention under the GDPR, more generally when profiling has legal or significant effects on data subjects (Article 22)[106] and especially when data subjects that are profiled are children (Recitals 38 and 71) given that Article 22(2) should be applied restrictively when the data subject is a child.[107] Thus, although behavioural profiling for age assurance effects all users of a digital service, in this analysis, we will focus on the situation where children are profiled for age assurance because of their higher level of protection under the GDPR. This processing activity will therefore have to meet the strict conditions that the GDPR imposes on the processing of children's personal data.

101 Santiago de Ampuero and Cristina Barón, 'Spanish Data Protection Agency's Guidance on Age Verification' (*Hogan Lovells*, 2 January 2024) <https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9Vap8ahmeIu1Hl17eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JAvAvaah9lF3dzoxprWhI6w%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true> accessed 1 August 2024.

102 Ofcom, Guidance on highly effective age assurance For Part 3 services (n 28).

103 Ofcom, 'Statement: Age Assurance and Children's Access' (16 January 2025) 21–22 <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/statement-age-assurance-and-childrens-access.pdf?v=388849> accessed 9 March 2025.

104 ibid 167.

105 European Data Protection Board, 'Statement 1/2025 on Age Assurance' (11 February 2025) 3 <https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-12025-age-assurance_en> accessed 9 March 2025.

106 Provisions and Recitals in the subsection 'Behavioural profiling as age assurance under the GDPR' are taken from the GDPR unless otherwise indicated.

107 Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (Wp251rev.01, 2018) 28 <https://ec.europa.eu/newsroom/article29/redirection/document/49826> accessed 29 July 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

Behavioural profiling for age assurance and data protection principles

Several data protection principles in Article 5 raise important considerations with respect to behavioural profiling and potentially higher standards when the processing involves children's personal data.[108] For instance, the transparency principle is difficult to fulfil because complex datafication practices, including behavioural profiling, can be challenging to explain to children. The privacy policies of TikTok, Meta, and Google, that is online platforms that we know engage in behavioural profiling for age assurance,[109] do not provide information tailored to children, if the information is provided at all.[110]

A data protection principle that generally seems to conflict with behavioural profiling for age assurance is the *data minimisation* principle (Article 5(1)(c); see also Article 25). It entails that data controllers use only necessary yet sufficient information.[111] This principle—especially in relation to the principle of purpose specification (Article 5(1)(b)—)does not seem to be followed, given that behavioural profiling is a data-driven method that is likely to involve processing of data more than what is essential for age estimation.[112] Data minimization should also be considered, given that privacy-friendly age assurance methods exist, for example, zero knowledge age assurance.[113] Zero-knowledge proof methods use cryptography to enable users to prove their age without providing any other information to the platform, as there is an independent third-party acting as an intermediary that relays only the required information.[114] CNIL in France has recommended this as a privacy-friendly method of age verification,[115] and the EDPB has recommended this method when there is a high risk to users' privacy.[116] It was stressed by the EDPB that it is important for age assurance to follow principles such as purpose limitation and data minimization, to ensure that the age assurance process does not result in further profiling of users for commercial or malicious purposes.[117] The principle of data minimization must be more strictly respected in the case where children's personal data are processed.[118]

When age is estimated based on inferred data, this may violate the *accuracy* principle, which states that personal data must be accurate and if not, they must be deleted and corrected immediately (Article 5(1)(d)). As explained in the subsection 'Advantages and disadvantages of behavioural profiling as age estimation', behavioural profiling for age assurance may be challenging in terms of how accurate the algorithmic analysis is, given the inherent vulnerabilities of AI systems. Since users may also not be aware that behavioural profiling for age assurance is taking place, let alone what the results are and whether the results are accurate, they cannot request deletion or correction themselves, and users are dependent on safeguards built in by platforms themselves. To what extent these safeguards exist and what they look like is unclear, though platforms like TikTok expressly provide an appeal mechanism if access to the platform or its functionalities is suspended because the user is believed to be below the minimum age.[119]

Further, when behavioural profiling is not transparent to users, including children, or results in inaccurate or even biased results (see the subsection 'Advantages and disadvantages of behavioural profiling as age estimation'), the processing also does not conform to the principle of *fairness* (Article 5(1)(a)).[120] The EDPB stated in the age assurance context, '*[t]he concept of transparency is fundamentally linked to fairness*' because if entities that conduct age assurance do not make it clear to the users the information processed for age assurance and the privacy impact of the same, such processing is unlikely to be fair or lawful.[121] It bears mention that fairness under the GDPR should not be

108 van der Hof, Lievens and Milkaite (n 61) para 4.

109 Diwanji (n 5); TikTok, 'Privacy Policy' (n 6); Google, 'Privacy & Terms' (n 7).

110 TikTok's and Google's privacy policy does mention that it uses behavioural profiling for the purpose of age assurance, see TikTok, 'Privacy Policy' (n 6); Google, 'Privacy & Terms' (n 7). Meta's data policy does not provide this information, see Instagram (n 51).

111 Moreover, such data should only be stored as long as is necessary for the specific purpose and hence deleted when no longer necessary (art 5(1)(e)), which may imply that when age has been estimated the personal data must be deleted again; see Case C-553/07 *College van burgemeester en wethouders van Rotterdam v M E E Rijkeboer* [2009] ECLI:EU:C:2009:293, para 33; Case C-136/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772, para 74.

112 5Rights Foundation (n 25) 32; UNICEF (n 25) 29.

113 Shaffique and van der Hof (n 2) 33–34; also referring to eg Commission Nationale Informatique & Libertés, 'Online Age Verification: Balancing Privacy and the Protection of Minors' (22 September 2022) <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors> accessed 13 November 2024.

114 eSafety Commissioner (n 46) 174.

115 Commission Nationale Informatique & Libertés (n 113).

116 European Data Protection Board, 'Statement 1/2025 on Age Assurance' (n 105) 9.

117 ibid 4.

118 Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (WP 202, 2013) 26 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> accessed 28 October 2024.

119 TikTok, 'Minimum Age Appeals on TikTok' (n 79); TikTok, 'Underage Appeals on TikTok' (n 79).

120 Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679 (n 107) 4–5.

121 European Data Protection Board, 'Statement 1/2025 on Age Assurance' (n 105) 7.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

interpreted only as transparency or procedural fairness, that is a process is fair.[122] Fairness can also be envisaged as substantive fairness, that is the outcome or consequence of a process is fair.[123] Regarding behavioural profiling, this means that not only should the processing of data for the profiling comply with the GDPR principles, but also that such processing should not result in unfair outcomes, for example, incorrect exclusion of users who are of sufficient age.

Lawfulness of behavioural profiling for age assurance

The principle of *lawfulness* (Article 5(1)(a)) entails that personal data can only be lawfully processed if the processing is based on one of the six exhaustive legal grounds in Article 6. Although it seems obvious to turn to Article 6(1)(b), that is data processing is necessary for the performance of a contract, since there is a contractual relationship between the digital service provider and user, this provision involves a Catch-22 situation. A contract within the meaning of Article 6(1)(b) must be legally valid based on the applicable national law,[124] and in many legal systems, minors (normally persons under 18) do not have the legal capacity to contract.[125] Therefore, to lawfully process personal data for the purpose of age assurance based on this legal ground, you must have already established whether the data subject is old enough to have legal capacity to contract, and thus have performed age assurance, to conclude a contract in the first place. Age assurance in the form of self-declaration, that is the user enters his or her age or date of birth in the registration process to check if they are old enough to use the service according to the terms and conditions, can be covered by this provision since it might fall under processing that is necessary in order to take steps at the request of the data subject *prior to entering into a contract* in Article 6(1)(b).[126] In the case of behavioural profiling as age assurance, however, the child user must already have an account and thus be in a contractual relationship with the digital service provider in order to process behavioural data for this purpose, and the Catch-22 remains. Similarly, though the data subject may also consent to data processing for the purpose of behavioural profiling as age assurance (Article 6(1)(a)), this legal ground is subject to the same Catch-22 problem as Article 6(1)(b). To request legally valid consent, you first need to know whether the data subject in question has reached the age of digital consent (Article 8), because otherwise parental consent is required. Moreover, consent is subject to strict conditions (such as that it must be freely given and informed,[127] see Articles 4(11) and 7), which may be difficult to satisfy, especially in the case of children.[128]

Moreover, there may be a legal obligation in EU or member state law based on which digital service providers must provide age assurance, for which processing of personal data is necessary (Article 6(1)(c)). As mentioned in the subsection 'The legal relevance of age assurance', the law may require persons to be of a certain minimum age to, eg access a service or perform a legal act, which means, or at least implies, that age assurance is required. In this case, Article 6(1)(c) provides a legal ground for the processing of personal data. In addition, a digital service provider may have a legitimate interest to process personal data for the purpose of age assurance (Article 6(1)(f)), even if no legal obligation in EU or member state law exists. For instance, a digital service provider may have stipulated in their general terms and conditions that access to the service is subject to a minimum age. The digital service provider can have a 'legitimate interest' in setting such a rule because the service may not be suitable for users of all ages. In that case, the processing of personal data may be necessary for the purpose of age assurance to determine whether a user is above the minimum age when, for example signing up for an account.

Both these legal grounds, that is 'legal obligation' (Article 6(1)(c)) and 'legitimate interest' (Article 6(1)(f)), can thus in principle provide a legal ground for age

122 Andreas Hauselmann and Bart Custers, 'Substantive Fairness in the GDPR: Fairness Elements for Article 5.1a GDPR' (2024) 52 Computer Law & Security Review 3 <https://doi.org/10.1016/j.clsr.2024.105942> accessed 28 October 2024.

123 ibid 4.

124 European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (Version 2.0, 2019) 6 <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 28 October 2024.

125 Martijn W Hesselink, 'Capacity and Capability in European Contract Law' (2005) 13 European Review of Private Law 491, 496 <https://doi.org/10.54648/erpl2005031> accessed 11 November 2024.

126 If age assurance is a legal obligation under EU or Member State law with which the digital service must comply with, the legal ground is art 6(1)(c). A contractual stipulation by a digital service provider, eg a minimum age requirement in their terms and conditions, is not covered by this legal ground; see Waltraut Kotschy, 'Article 6 Lawfulness of Processing' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 331–32 <https://doi.org/10.1093/oso/9780198826491.003.0035> accessed 14 April 2025.

127 See also the subsection 'Behavioural profiling for age assurance and data protection principles' with respect to transparency.

128 See also Article 29 Data Protection Working Party, Opinion 02/2013 on Apps on Smart Devices (n 118) 26, which regarding consent states with respect to another form of behavioural profiling: 'data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

assurance by digital service providers. However, both provisions are conditional to, among others, the extent to which the processing of personal data is proportionate and whether the method used is effective. First, in the case of both legal grounds, it is important that the processing is 'necessary' for the specific purpose, that is age assurance, a requirement which is interpreted restrictively.[129] The test that age assurance must satisfy under this requires that 'the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects'.[130] Meaning that '[i]f there are realistic, less intrusive alternatives, the processing is not "necessary"'.[131] The reference to fundamental rights concerns more specifically also the rights of children, in which case Article 6(1)(f) moreover specifically provides for the protection of children's rights in line with Recital 38. As we have seen earlier (see the subsections 'The relation between behavioural profiling as age estimation and commercial profiling' and 'Advantages and disadvantages of behavioural profiling as age estimation'), age assurance based on behavioural profiling is a method that is data-driven and is expected to process extensive data and especially more data than other privacy-friendly methods that exist or are being developed.[132] Moreover, behavioural profiling as age assurance is a method of age *estimation* and thus only estimates whether someone has reached the required minimum age. The results may not be accurate, and the method not as effective—at least not by itself—as potentially other methods that, again, may also be more privacy friendly.[133] It is therefore doubtful that, depending on the purpose, personal data can be lawfully processed on either of these legal grounds.

Even if the processing is necessary, for Article 6(1)(f) to apply, the legitimate interest of the digital service provider must also be balanced against the interests and fundamental rights of data subjects to determine whether the impact is proportionate, given also the Article 5 data protection principles and obligations for data controllers that apply. The subsection 'Behavioural profiling for age assurance and data protection principles' of this article already pointed out that behavioural profiling for age assurance may not comply with the principles of transparency, data minimization, accuracy, and fairness. Other relevant factors in the balancing test are, among others, how the processing impacts users (eg behavioural profiling may result in exclusion of or discrimination against users), the nature of the data that is processed (eg behavioural profiling may involve the processing of sensitive or private data), the context and methods of processing (eg behavioural profiling may involve processing of high volumes of data, and the combination of data sets, and have consequences related to the vulnerability of the data subject).[134] In particular, children deserve a high level of protection regarding the processing of their personal data, because not only may they lack understanding of the consequences of the processing (Recital 38), but those consequences may also be greater in their case. If behavioural profiling as age assurance is not effective enough, children who are not the minimum age required by many online platforms still use them, even if these platforms are not appropriate or safe for them. In practice, this is indeed the case for many, if not all, online platforms used by children.[135] This factor should be considered in the balancing test where the child's best interest (Article 3 UN CRC; Article 24 Charter) is a high priority.[136] In principle, profiling children is not perceived as in the best interest of the child.[137] Finally, the balancing test must take into account the reasonable expectations of the data subject (Recital 47). If data subjects do not have information about, or do not sufficiently understand, the data processing, this may contribute to them not reasonably expecting it. What someone should reasonably expect also depends on age: adults are expected to have different expectations than children, and older teenagers may have different expectations than younger teenagers or children.[138] Thus, while age assurance may constitute a legitimate interest of companies for data processing, the necessity test and balancing test based on the

129 European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects (n 124) 8.

130 Case C-252/21 *Meta Platforms Inc v Bundeskartellamt* [2023] ECLI:EU:C:2023:537, para 108.

131 European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects (n 124) 25.

132 Shaffique and van der Hof (n 2) 33–34.

133 ibid.

134 European Data Protection Board, 'Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR' (Version 1.0, 2024) paras 39–45 <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> accessed 10 October 2024; see also *Meta Platforms Inc* Case (n 130) para 116.

135 Thorn, 'Online Grooming: Examining Risky Encounters amid Everyday Digital Socialization Findings from 2021 Qualitative and Quantitative Research among 9-17-Year-Olds' (April 2022) 27, <https://info.thorn.org/hubfs/Research/2022_Online_Grooming_Report.pdf> accessed 28 October 2024.

136 European Data Protection Board, Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR (n 134) para 94.

137 ibid para 95; *Meta Platforms Inc* Case (n 130) para 111.

138 European Data Protection Board, Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR (n 134) paras 53–54.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

weighted relevant factors may depend on the design and implementation of the age assurance method, which, in this case, is behavioural profiling for age assurance, and may still lead to the conclusion that the data processing is disproportionate.

The conclusion of the analysis of Article 6 is that data processing for age assurance must be based on Article 6(1)(c) if there is a legal obligation or Article 6 (1)(f) if there is no such legal obligation but the digital service provider nevertheless has a legitimate interest. However, it is doubtful whether behavioural profiling as age assurance passes the necessity test of both provisions and the balancing test of Article 6(1)(f).

Behavioural profiling as age assurance and Article 22 GDPR

If behavioural profiling as age assurance complies with data protection principles and in particular is carried out on the basis of and within the conditions of the legal ground of Article 6(1)(c) or (f), arises the question of whether this form of profiling is in line with Article 22. Article 22 provides a prohibition on completely automated decision-making, including automated profiling, if it involves (the likelihood of) legal or similarly significant effects for the data subject,[139] the impact of which may be greater for vulnerable data subjects like children.[140] Behavioural profiling as age assurance may involve such effects. For instance, *Google* restricts user accounts if Google 'learns' that the user is not of the minimum age required.[141] Google's privacy policy explicitly states that owing to legal obligations dictating that users be of sufficient age, Google analyses 'information about your activity in our services, both when you're signed in to a Google Account or signed out, and use machine learning technology to determine if you are likely over 18'.[142] Therefore, the decisions taken based on behavioural profiling implemented by Google through machine learning can have the effect of users not being able to access their Google accounts. This can produce significant effects given the large and multi-faceted roles such platforms play in users' lives, for example, by affecting the freedom of expression of users.[143]

Thus, behavioural profiling may result in the cancellation of the contract with the digital service provider and deletion of a user's account.[144] This can be a purpose of age assurance, as a user may not have the minimum age to create an account according to the terms and conditions of a digital service provider. But if this happens after previous age assurance performed by the provider was ineffective, then a user may have already built a profile and created content that, with the deletion of the account, are also removed. Here, it should also be considered that age assurance is the responsibility of the provider, who can be expected to use adequate methods. Moreover, exclusion of or discrimination against data subjects may be significant effects of behavioural profiling for age assurance.[145] A user who does have the required minimum age may be unfairly excluded because their age is incorrectly estimated. Moreover, inaccurate behavioural profiling results can be discriminatory (see the subsection 'Advantages and disadvantages of behavioural profiling as age estimation').

If behavioural profiling as age assurance has these effects, it is prohibited unless the exceptions of Article 22(2) apply. Two of these exceptions, that is 'necessary for the performance of or entering into a contract' (a) and 'explicit consent' (c), are subject to the Catch-22 situations already explained in the subsection 'Lawfulness of behavioural profiling for age assurance', with respect to Article 6(1)(a) and (b). The third exception is that behavioural measures for age assurance are authorized by EU or Member State law. As far as we know, such a legal authorization does not exist.

More specifically, with respect to children, both Recitals 38 and 71 point to a higher level of protection of children. Hence, the exceptions of Article 22(2) must in their case be interpreted restrictively, which means the exceptions should only be relied upon if in the best interest of the child (Article 3 UN CRC; Article 24 Charter).[146] Despite the fact that age assurance may be in the interest of children, it is inconceivable that the legislator would consider an Article 22(2)(b) legal provision to allow behavioural profiling as age assurance

139 Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (n 107) 19–20.

140 van der Hof, Lievens and Milkaite (n 61) para 24.

141 Google, 'Age Requirements on Google Accounts' (*Google Account Help*) <https://support.google.com/accounts/answer/1350409?hl=en&sjid=17906494263792731842-EU#zippy=%2Ceurope> accessed 30 July 2024; Google, 'Update Your Account to Meet Age Requirements' (*Google Account Help*) <https://support.google.com/accounts/answer/1333913?sjid=17906494263792731842-EU> accessed 30 July 2024.

142 Google, 'Privacy & Terms' (n 7).

143 European Data Protection Board, 'Statement 1/2025 on Age Assurance' (n 105) 8.

144 Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (n 107) 21.

145 ibid.

146 van der Hof, Lievens and Milkaite (n 61) para 26; Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (n 107) 28.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

within Article 22(1), given the potential breach of Article 5 data protection principles (see section 'Behavioural profiling for age assurance and data protection principles').

Behavioural profiling as age assurance under the DSA

Article 28[147] places an obligation on online platforms to protect children online. It is specifically provided in Article 28(2) that if a user is known to be a minor with reasonably certainty, then the user should not be subjected to targeted advertisements based on profiles developed using personal data. Targeted advertisements based on profiles developed using special categories of data as defined in Article 9(1) GDPR are prohibited for all users (Article 26(3)). Moreover, the DSA puts restrictions on profiling-based recommender systems by very large online platforms and very large online search engines (Article 38). However, these prescriptions are in the context of profiling for advertisement purposes and not directed at behavioural profiling (though they can be interconnected as discussed in the subsection 'The relation between behavioural profiling as age estimation and commercial profiling').

While the DSA does not specifically regulate behavioural profiling, Article 28(1) may have an impact on such profiling by providing that online platforms should employ 'appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors' if they can be accessed by children. The DSA does not specify what constitutes a high level of privacy, safety and security. Recently, the European Commission conducted a call for evidence to formulate guidelines for the protection of minors online as per Article 28(4) DSA, which seeks to *inter alia* develop good practices in relation to age assurance,[148] which guidance should hopefully be released in 2025. However, it is reasonable to conclude that even if profiling of children is done for non-commercial purposes, such as assessing age, it should still be subject to the strictest scrutiny, particularly given the various risks associated with behavioural profiling as discussed in the subsection 'Advantages and disadvantages of behavioural profiling as age estimation' and our legal analysis of behavioural profiling as age assurance under the GDPR in the subsection 'Behavioural profiling as age assurance under the GDPR'. The wording of Article 28(3), which states that in order to comply with Article 28, online platforms may not process further personal data to determine whether a user is a minor, gives further credence to this interpretation. While the exact meaning of Article 28(3) is not clear, it is possibly an indication that age assurance should be privacy-friendly.[149] It is expected that the European Commission's guidelines will throw more light on this aspect as well.

Behavioural profiling as age assurance under the AVMSD

The AVMSD contains provisions more directly related to behavioural profiling. Articles 6a and 28b,[150] respectively, require media service providers and video-sharing platforms to take appropriate measures to protect minors from harmful content, including age verification tools. However, the personal data of minors processed to implement such protection measures may not be 'processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising' (Articles 6a(2) and 28b(3)). Therefore, this provision means that media service providers and video-sharing platforms are legally obliged not to use the data of children processed for behavioural profiling for commercial purposes, even though behavioural profiling for age assurance purposes, as such, is not specifically excluded. The Online Safety Code published by Ireland's media regulator (Coimisiún na Meán) confirms this view present in Article 28b(3) AVMSD, and clarifies that age verification tools in this context include age estimation methods as well.[151] Notably, such a restriction on utilizing personal data for commercial purposes is only mentioned in the context of data of minors, meaning that no similar stipulation is present in AVMSD as regards data of other users. However, behavioural profiling would naturally involve processing data of adults as well. Thus, to assess whether such data can be used for commercial profiling, one would have to rely on the GDPR provisions elaborated in the

147 Provisions and Recitals in the subsection 'Behavioural profiling as age assurance under the DSA' are taken from the DSA unless otherwise indicated.

148 European Commission, 'CALL FOR EVIDENCE FOR AN INITIATIVE (without an impact assessment), Digital Services Act—guidelines to enforce the protection of minors online' (31 July 2024) 2 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14352-Protection-of-minors-guidelines_en> accessed 22 October 2024; The European Commission has also established a Task Force on Age Verification to 'cooperation with national authorities of Member States with expertise in the field to identify best practices and standards in age verification', see European Commission, 'Digital Services Act: Task Force on Age Verification' (n 14); European Commission, 'Second Meeting of the Task Force on Age Verification' (n 14).

149 Livingstone and others (n 12) 32.

150 Provisions and Recitals in the subsection 'Behavioural profiling as age assurance under the AVMSD' are taken from the AVMSD unless otherwise indicated.

151 Coimisiún na Meán, 'Online Safety Code' (October 2024) 12-13 <https://www.cnam.ie/app/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf> accessed 9 March 2025.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

subsection 'Behavioural profiling as age assurance under the GDPR'.

Behavioural profiling as age assurance under the AI Act

As behavioural profiling utilizes AI, it is relevant to analyse how recent legislation governing AI, that is, the AI Act, regulates this form of age assurance. Broadly put, the AI Act is an EU regulation that lays down requirements for different types of AI systems and AI practices, based on their risks, capabilities, and use cases. The use of AI for behavioural profiling does not appear to fall under one of the prohibited AI practices as laid down in Article 5.[152] However, the AI Act can still be applicable to behavioural profiling in different ways.

Behavioural profiling for age assurance as a high-risk AI system

There are several obligations imposed by the AI Act when it comes to high-risk AI systems, including relating to risk management and transparency. Article 6 provides the rules for the classification of high-risk AI systems.[153] Broadly put there are two ways in which an AI system can be considered high-risk: (i) the AI system is governed by one of the laws mentioned in Annex I and it is mandated to undergo third-party conformity assessment to be made available in the EU (Article 6 (1)), or (ii) the AI system is included in the list of AI systems referred in Annex III (Article 6(2)).

Based on Annex III(1)(b), behavioural profiling can be considered as high-risk AI system if (a) 'biometric data' of an individual are used by the AI, (b) for a 'biometric categorisation system', and (c) such categorization is done on the basis of the individual's sensitive or protected attributes. To analyse the applicability of these provisions to behavioural profiling, it is relevant to delve deeper into the meaning of these elements.

(a) Biometric Data: Article 3(34) defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person'. There are two key aspects to this definition. First, the processing of 'behavioural characteristics' of a person is also considered biometric data, which is particularly relevant to behavioural profiling, where online user behaviour is analysed. Secondly, while the definition of biometric data in Article 4(14) GDPR requires that personal data must be involved in the unique identification of an individual for the personal data to qualify as biometric data, this requirement is not present in the AI Act.

Behavioural data that is used for biometric purposes, also termed as 'behavioural biometrics', analyses how humans interact with devices using functionalities' features such as keystroke dynamics and touch dynamics.[154] For instance, how a person uses the touchscreen of their phone can be monitored to ascertain whether the correct and authenticated person has access to a mobile application.[155] Similarly, the analyses of email patterns, mouse actions, etc, of a person can be used in behavioural biometrics.[156] Applications for behavioural biometrics include online and mobile banking to identify that only authorized parties access bank accounts.[157]

As discussed in the subsection 'Behavioural profiling as age assurance', similar parameters, including mouse and keyboard usage, are also used for age assurance-related behavioural profiling. Specifically in the context of online user behaviour, it has been argued that analysing a person's online activities, such as their 'specific usage of devices or contents searching patterns', should fall under behavioural data and hence biometric data.[158] Therefore, it can be claimed that under the AI Act, data processed in the context of behavioural profiling squarely fall under the category of 'biometric data'. This is particularly so because, as mentioned earlier, the AI

152 Provisions and Recitals in the subsection 'Behavioural profiling as age assurance under the AI Act' are taken from the AI Act unless otherwise indicated.

153 High-risk systems must comply with specific rules, including requiring a risk management system (art 9), maintaining of records (art 12) and ensuring appropriate levels of accuracy, robustness and cybersecurity (art 12). These obligations may apply to various operators associated with high-risk AI systems, such as providers, deployers, importers, and distributors of the systems (arts 16–27).

154 Mohamed Amine Ferrag and others, 'Taxonomy of Biometric-based Authentication Schemes for Mobile Computing Devices' (2018) 2018 3rd international conference on pattern analysis and intelligent systems 1, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8598491&casa_token=tdx6DfU7L-QAAAAA:pn5RveXaEsjKH1le2MvAKs3p1Eb4cHZ8z0jSAgZspOx5VP8j18ovj2Vb_h_IEdJH_KySSSD-o2Y&tag=1> accessed 30 August 2024.

155 Mario Frank and others, 'Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication' (2012) 8 IEEE transactions on information forensics and security 136, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6331527> accessed 30 August 2024.

156 Roman Yampolskiy and Venu Govindaraju, 'Taxonomy of Behavioural Biometrics' (2010) Behavioral Biometrics for Human Identification: Intelligent Applications 1 <https://www.researchgate.net/publication/254217766_Taxonomy_of_Behavioural_Biometrics> accessed 30 August 2024.

157 Ayelet Biger-Levin, 'What Is Behavioral Biometrics?' (*BioCatch*) <https://www.biocatch.com/blog/what-is-behavioral-biometrics#:~:text=Behavioral%20biometrics%20analyzes%20a%20user's,identifying%20fraud%20and%20identity%20theft> accessed 30 August 2024.

158 Ján Matejka and others, *Biometric Data and Its Specific Legal Protection* (Praha: Institute of State and Law of the Czech Academy of Sciences 2020) 43 <https://www.researchgate.net/profile/Jan-Matejka-5/publication/340004915_Biometric_Data_and_Its_Specific_Legal_Protection/links/65c25f0034bbff5ba7f091a0/Biometric-Data-and-Its-Specific-Legal-Protection.pdf> accessed 30 August 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

Act does not require these data to enable the unique identification of a person, as in the GDPR.

(b) Biometric categorization system: Article 3(40) defines a biometric categorization system as AI systems whose purpose is to classify people into certain categories based on their biometric data. Therefore, if behavioural profiling involves processing biometric data, and if these data are used to classify users based on their age groups, it can be said that AI-based behavioural profiling is a biometric categorization system.

(c) Sensitive attributes: Whether a biometric categorization is based on sensitive or protected attributes depends on the facts and circumstances surrounding the behavioural profiling. Article 3(37) adopts the definition of 'special categories of personal data' or 'sensitive data' from Article 9(1) GDPR. Generally speaking, personal data relating to race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (for uniquely identifying a person), health, sex life, and sexual orientation are classified as sensitive data in Article 9(1) GDPR. While at first glance behavioural profiling does not appear to effect biometric categorization based on sensitive attributes, this is far from certain. For instance, if the AI system draws an inference that users who hold certain political or philosophical beliefs are more likely to be of a certain age. Further, the European Court of Justice's broad interpretation of sensitive data[159] and the inferences that can be made from such data[160] could make it more likely for behavioural profiling to be viewed as using sensitive attributes. Though it might be practically unlikely that AI systems for age assurance are trained in this manner, this is still an issue that merits consideration. Finally, even where an AI system is classified as high-risk under Article 6(2), Article 6(3) provides certain derogations from this classification. However, such derogations do not apply when the AI system creates user profiles, as in the case of behavioural profiling.

Article 50 transparency requirements and general-purpose AI models

If behavioural profiling amounts to biometric categorization as described above, then requirements fastened by Article 50 may apply even if the process does not use sensitive data. Article 50 imposes transparency obligations with respect to certain AI systems that may be generative AI, create deep fakes, etc, and one such AI system mentioned in the provision is a biometric categorization system. Deployers of such systems should inform users that such a system is being used (see Article 50(3)). Article 50 thus goes hand in hand with the principle of transparency and transparency obligations in the GDPR that apply to the processing of personal data by such systems (see the subsection 'Behavioural profiling as age assurance under the GDPR'). Finally, if a general-purpose AI model[161] is used to make profiling decisions, requirements related to such models may also be relevant.[162]

Conclusion

The growing emphasis in policy and legislation on protecting the rights and wellbeing of children requires online platforms to know who of their users are children (or adults for that matter) and adapt services or functionalities to ensure that they are safe for (groups of) children or (groups of) children cannot use them if safety cannot be guaranteed. Although there are different forms of age assurance, that is self-declaration, age estimation, and age verification, important legal provisions for digital service providers cannot be met without age verification, even when it is not explicitly required by law. For example, the GDPR and DSA require a higher level of protection for (groups of) children that can only be provided if you know which of your users fall within the relevant age groups. This is also the reason why the focus on developing and implementing privacy-friendly online age verification methods is growing.

In contrast, behavioural profiling for age assurance used by at least some online platforms raises privacy and security concerns for users, and our analysis shows that these are not unjustified. What is more, behavioural profiling as age assurance is problematic in a legal sense. Under the GDPR, this form of profiling does not (always) meet the data protection principles of data minimization, transparency, accuracy, and thus fairness. In the sense of lawfulness of data processing, there may possibly be a legal obligation or legitimate interest to process data for age assurance, but behavioural profiling for age assurance is unlikely to be a proportionate and

159 *Bodil Lindqvist*, Case C-101/01, [2003] ECR I-12971 (ECLI: EU:C:2003:596).

160 *OT v Vyriausioji tarnybinės etikos komisija*, Case C-184/20 [2022] ECLI: EU:C:2022:601.

161 See AI Act, art 3(63) for definition of general-purpose AI model.

162 These requirements include maintaining technical documentation and having a policy to comply with the copyright regime (art 53). If such models are classified as posing systemic risk under arts 51 and 52, further obligations regarding risk assessment and mitigation and an adequate level of cybersecurity must be met (art 55).

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

effective way of age assurance and therefore does not meet the requirements of the GDPR nor the DSA. The main concern in this regard is also that if deemed acceptable, behavioural profiling can provide fertile ground for platforms to leverage monitoring of online user behaviour for commercial profiling of users. Moreover, behavioural profiling as age assurance is likely to be a high-risk system under the AI Act if sensitive attributes are used. Almost certainly, though—similar to the GDPR—transparency requirements apply to this form of behavioural profiling as a 'biometric categorisation system'. Although this relatively frictionless method, as part of their broader profiling practices, is attractive to the industry, it is essential that users themselves are involved in verifying their age using privacy and user-friendly methods soundly developed based on the legal requirements for age assurance itself. At the outset, digital service providers have to ensure better transparency regarding the behavioural profiling employed by them, so as to enhance user awareness and to facilitate a critical discussion on the appropriateness of this practice.

Finally, in cases where age verification is required by legislation, it might be important to introduce friction and make the user part of the decision-making process by allowing them to verify in a secure, privacy- and user-friendly way that they have reached a minimum (or maximum)[163] age to use certain digital services or functionalities.[164] Using self-declaration or age estimation in place of age verification, for the purpose of reducing user friction, may thus not be a justified measure. Moreover, using age verification when it is required can ensure that age assurance complies with the law, unlike now, with behavioural profiling for age assurance. In other words, meeting legal age verification obligations does trigger legal obligations for using age assurance methods that may be difficult to comply with by platforms from a user friendliness perspective, which does not mean that adhering to legal requirements and ensuring the safety of users should be compromised.

Conflict of interest. The authors declare that they have no known competing financial interests or personal relationships or other conflict of interest that could have appeared to influence the work reported in this paper.

https://doi.org/10.1093/idpl/ipaf012

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaf012/8327959 by guest on 19 May 2026

163 Generally age related restrictions impose a minimum age for users, but certain platforms could also impose a maximum age, for instance to create child-friendly spaces which adults cannot access. See Shaffique and van der Hof (n 2) 23.

164 In 2024, EU Regulation 910/2014 establishing the European Digital Identity Framework entered into force and requires EU Digital Identity Wallets to be implemented in EU Member States in 2026 (art 5a). EU digital wallets can become secure and privacy friendly instrument for age verification if they become available to children. See Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [2024] OJ L2024/1183.