Statement

Statement 1/2025 on Age Assurance

Adopted on 11 February 2025[1]

The European Data Protection Board has adopted the following statement:

1. BACKGROUND AND PURPOSE OF THIS STATEMENT

1. The European regulatory framework calls for the increased protection of children in the digital environment. For example, the Audiovisual Media Services Directive[2], which Member States have transposed into their national laws, highlights the possibility to implement age verification measures (Articles 6a and 28b), the GDPR introduces minimum age requirements for consenting to the processing of personal data in the context of information society services (Article 8), the Digital Services Act[3] references age verification as a risk mitigation measure (Article 35(1)), and a number of Member States have implemented minimum age requirements for performing legal acts, exercising certain rights or accessing certain goods and services into their own national laws.

2. In addition, different national and European initiatives, such as Better Internet for Kids (BIK+), identify age assurance as one solution to improve children's well-being online through a safe, age-appropriate digital environment in line with the European Digital Rights and Principles[4].

3. Based on the definition provided in the research report *Mapping age assurance typologies and requirements*[5], this document will use "age assurance" as '*the umbrella term for the methods that are used to determine the age or age range of an individual to varying levels of*

[1] Minor corrections to the formatting of this document were made on 24 February 2025
[2] 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, https://eur-lex.europa.eu/eli/dir/2018/1808/oj
[3] 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) , https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[4] Better Internet for Kids, Guide to age assurance, https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest
[5] Raiz Shaffique, M., & van der Hof, S. (2024). Mapping age assurance typologies and requirements. Research report, Part of the Better Internet for Kids (BIK) project coordinated by European Schoolnet (EUN) and commissioned by the European Commission.

confidence or certainty'. The same report mentions three primary categories of age assurance: age estimation, age verification and self-declaration.

4. Age assurance poses specific risks to data protection with the potential to adversely impact not only natural persons' right to the protection of their personal data, but also other rights and freedoms[6] such as the right to non-discrimination, the right to the integrity of the person, the right to liberty and security, and the right to free expression and information.

5. In recognition of the importance of a consistent approach at EU level on the topic of age assurance, the EDPB wishes to provide specific guidance and high-level principles stemming from the GDPR that should be taken in consideration when personal data is processed in the context of age assurance.

6. The proposed principles seek to reconcile the protection of children and the protection of personal data in the context of age assurance.

7. Priority has been given to address the requirements concerning the main principles stated in Article 5 GDPR (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality, integrity, and accountability), and to ensure these data protection principles are properly implemented and remain robust over time, as set out under Article 25 GDPR "Data protection by design and by default" and Article 32 GDPR "Security of processing".

8. This statement is focused on the principles applicable to different online use cases, including when a minimum age is prescribed by law or otherwise for buying products, for using services that may harm children or for performing legal acts; and when there is a duty of care to protect children (for example, to ensure that services are designed or offered in an age-appropriate way).

9. The EDPB may also consider issuing – whenever relevant and in other documents – additional guidance on specific use cases.

2. PRINCIPLES TO DESIGN GDPR-COMPLIANT AGE ASSURANCE

2.1 Full and effective enjoyment of rights and freedoms

Age assurance must respect the full complement of natural persons' fundamental rights[7] and freedoms, and the best interests of the child should be a primary consideration for all parties involved in the process.

[6] About the potential impact of age assurance on rights and freedoms, see, e.g.: "Roadmap for age verification" (Australian eSafety Commissionner, 2023) https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf?v=1731644498261, "A safe internet by default for children and the role of age verification" (AEPD, 2024) https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf or "Trustworthy Age Assurance?" a study commissioned by the Greens/EFA Cluster on Green and Social Economy at the European Parliament (2024) https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance

[7] In particular, the Universal Declaration of Human Rights, the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, and the UN Convention on the Rights of the Child.

10. When implementing age assurance, service providers should ensure that they consider not only the impact on the right to the protection of personal data, but on all fundamental rights of natural persons.

11. In the specific case of children, the best interests of the child[8] should be a primary consideration for all parties involved in age assurance. It is important to note that there is no hierarchy in considering the best interests of the child, and regard should be had for all children's rights[9] including their right to the protection of personal data, to protection from violence and all other forms of exploitation to access information from a variety of sources and to have their views given due weight.

2.2 Risk-based assessment of the proportionality of age assurance

Age assurance should always be implemented in a risk-based and proportionate manner that is compatible with natural persons' rights and freedoms.

12. Service providers should adopt a risk-based approach when designing and operating their services. The necessity and proportionality of using safety measures such as age assurance should be demonstrated, taking into account the associated risks. The necessity could be demonstrated by conducting an assessment[10] to identify and evaluate the risks that a particular service poses for children[11], such as exposure to harmful contact or content. As part of this assessment, service providers may also consider the rights of children, the opportunities provided by the digital environment, the views of the children as well as their evolving capacities in order to ensure age-appropriate participation[12].

13. Service providers must also respect their users' rights and freedoms, including the right to the protection of their personal data, balancing these with the need for safety measures which should always be the least intrusive of those available and which should always be effective. In many cases, age assurance poses a high risk to the rights and freedoms of data subjects, which would therefore require that a Data Protection Impact Assessment ("DPIA", Article 35 GDPR) be conducted before processing, taking into account the nature, scope, context and purposes of the processing. The DPIA should include a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller. It should also contain an assessment of the necessity and proportionality of the processing, identify risks arising from processing personal data for the purpose of age assurance and contain measures to mitigate those risks[13].

---

[8] The UN Committee on the Rights of the Child has clarified that the best interest's principle *'is aimed at ensuring both the full and effective enjoyment of all the rights recognized in the Convention and the holistic development of the child'*. General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1), https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf

[9] General Comment No. 25 (2021) on children's rights in relation to the digital environment, OHCHR, March 2021.

[10] For example, a Child Rights Impact Assessment ("CRIA"), which may or may not be part of a DPIA.

[11] Experts in the field of children's rights have highlighted the benefits of using Child Rights Impact Assessments (CRIA) as an effective tool *'for translating the Convention [on the Rights of the Child] and its Article 3, on giving priority to the child's best interests, into practice in a concrete, structured manner'* (in Mukherjee, S., Pothong, K., & Livingstone, S. (2021). Child Rights Impact Assessment: A tool to realise child rights in the digital environment. London: 5Rights Foundation). Furthermore, the UN Committee has called on States to mandate the use of CRIAs to embed children's rights into the regulation and design of the digital environment.

[12] General Comment No. 25 (2021) on children's rights in relation to the digital environment, OHCHR, March 2021.

[13] EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/items/611236/en

14. The DPIA should guide the design and implementation of appropriate technical and organisational measures for data protection compliance. This risk-based approach is crucial when balancing the potential interference with natural persons' rights and freedoms against the intended objective in this particular context, namely children's safety. The scope, extent, and intensity of this interference in terms of impact on rights and freedoms must always be carefully assessed[14]. For example, a service provider processing personal data to check the age of all their users when accessing all their content or services, even when the content or services are suitable for all audiences and devoid of any risk, would not pass the necessity and proportionality tests.

2.3 Prevention of data protection risks

Age assurance should not lead to any unnecessary data protection risks for natural persons. In particular, age assurance should not provide additional means for service providers to identify, locate, profile or track natural persons.

15. Service providers and any third party involved in age assurance should implement effective measures and safeguards to prevent this process from causing unnecessary data protection risks such as those resulting from identifying, locating, profiling, or tracking natural persons. The processing of personal data for age assurance should not provide additional means to fulfil purposes unrelated to the age assurance itself. This requires the selection of age assurance approaches that fully comply with the principle of data protection by design and by default (see section 2.8) and implementing measures that guarantee the principle of fairness, ensuring that personal data are not processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to data subjects.

16. For example, a natural person required to verify their age to access adult content would not expect the service provider to use age assurance to determine their identity or precise geographical location or to monitor, evaluate or infer personal aspects of their identity. This fact is particularly relevant for compliance with the data protection principles under Article 5(1), including fairness, transparency and purpose limitation, and the rules under Article 6(4) relating to subsequent uses of personal data. Similarly, following the principles of purpose limitation and data minimisation under Article 5(1), the age assurance process should not enable the further targeting or profiling of users, including for both commercial (e.g. personalised advertisements) and malicious targeting (e.g. grooming, bullying, stalking or harassment). The EDPB recalls that, under Recital 75, there may be particular risks to data protection rights when personal data relates to vulnerable natural persons, in particular of children. In general, it should not be possible to learn more than necessary about a natural person and their actions by profiling this person based on the information used in the age assurance process. This should be ensured, to the greatest extent possible, also in the event of a data breach.

17. Power imbalance situations should be avoided to prevent service providers from forcing individuals to face unnecessary data protection risks due to their lack of agency[15]. When this

[14] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] For example, when data subjects face automated decision making without proper redress mechanisms or when consent cannot be freely given. The "Imbalance of power" concept is discussed in the EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay

is not possible, these situations should be recognised and accounted for with suitable countermeasures[16]. For example, viable alternatives to prove their age should be provided to users who cannot or do not wish to use a specific method of age assurance. Furthermore, service providers should regularly assess whether the selected methods and technologies, including those provided by third parties, are functioning in line with their purposes and adjust them to ensure fairness in the processing. Third parties involved in age assurance should also seek to support service providers in complying with their obligations, by not introducing unnecessary data protection risks and by notifying any relevant changes to their policies, designs, services, etc. in a timely manner.

2.4 Purpose limitation and data minimisation

Service providers and any third party involved in age assurance should only process the age-related attributes that are strictly necessary for their specified, explicit and legitimate purpose.

18. In most cases, the purpose of age assurance is to make age-related access control decisions, prevent online harm for children, offer an appropriate design or experience according to age, etc. Regardless of the use case, the purpose of the personal data processing should be specific and explicit (Article 5(1)(b) GDPR). Once personal data are collected, they shall not be further processed or combined with additional data in a way that is incompatible with those purposes. Technical measures such as Privacy Enhancing Technologies ("PETs") should be used to limit the possibility of repurposing personal data. Organisational measures, such as policies and contractual obligations, which limit the reuse of personal data,[17] should also be deployed.

19. An age-related attribute is any attribute indicating that a natural person is a certain age, over or under a certain age or within an age range. The purpose specification will determine the relevant and necessary age-related attributes to be collected. Doing this will also allow the controller to assess the proportionality of the age assurance process. The advantages resulting from this process should not be outweighed by any disadvantages concerning the exercise of fundamental rights[18] (see section 2.2 above).

20. The controller should therefore only collect personal data that are necessary, adequate, and relevant for the purposes that are intended to be served. In this way, data minimisation helps to substantiate and operationalise the principles of necessity[19] and proportionality. For example, the service provider may only need to know whether the user is over or under an age threshold. This could be implemented by a tokenised approach based on the participation of a third-party provider, in which the service provider only sees the functional result of the

Models Implemented by Large Online Platforms (section 4.2.1.3), https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

[16] From the EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (section 2.3), Version 2.0, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[17] From the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[18] From the EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf

[19] From the EDPS toolkit for Assessing the necessity of measures that limit the fundamental right to the protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf

age assurance process (e.g. 'over' or 'under' the age threshold)[20]. Different approaches may be relevant when the service provider needs to know if the user is within a particular age range or born in a specific year.

2.5 Effectiveness of age assurance

Age assurance should demonstrably achieve a level of effectiveness adequate to the purpose for which it is carried out.

21. The means by which age assurance is carried out should be adequate to achieve the purpose of the processing. In particular, the effectiveness of any legally mandated age assurance measure should be considered as a precondition to satisfy the principles of necessity[21] and proportionality[22].

22. The effectiveness of age assurance should be evaluated on several aspects, including:

a) Accessibility. Age assurance should be broadly accessible for natural persons to verify their age or prove they meet an age-related requirement. When certain categories of individuals are at risk of being discriminated against by a specific age assurance method, for example because they do not own a suitable identity document or mobile phone or because of a disability, alternative methods for age assurance should be made available, when reasonably possible, with adequate levels of privacy, safety and security. Age assurance solutions should also comply with any applicable legislation on accessibility[23].
b) Reliability. According to the accuracy principle (Article 5(d) GDPR), any method whose purpose is to determine whether a natural person meets an age-related requirement should provide an adequate and consistent level of accuracy when determining whether or not they meet said requirement. Appropriate redress mechanisms should be made available, particularly when users can be significantly affected by automated decision-making, such as when their age-related attributes have not been properly established (see section 2.7 below).
c) Robustness. Age assurance should be able to deal with unexpected situations and resist reasonably likely attempts to trick or bypass the system. It should be noted that robustness has little meaning in the context of the self-declaration of an age-related attribute, since the reliability of such method depends mostly on the goodwill of the user[24].

[20] A third-party provider performs an age check and provides the user with an "age token" that the user can present to the service provider without needing to prove their age again. The age token may contain different user's attributes and about when, where or how the age check was performed.

[21] EDPS toolkit for Assessing the necessity of measures that limit the fundamental right to the protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf

[22] Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf

[23] For example, the accessibility of public sector websites and mobile applications and the accessibility of products and services are provided for by the Web Accessibility Directive (WAD) and the European Accessibility Act (EAA) respectively. Age assurance solutions must make sure they confirm to these legislations, by meeting the requirements of the harmonised European standard on the Accessibility requirements for ICT products and services, EN 301 549 v3.2.1.

[24] The EDPB has previously expressed serious doubts as to the effectiveness of self-declaration as a method of age verification within the context of high-risk processing in the Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf

In addition, service providers implementing age assurance and any third parties involved in the process should be able to demonstrate its effectiveness and be transparent about the means by which they reach appropriate levels of accessibility, reliability and robustness (see section 2.10).

2.6 Lawfulness, fairness and transparency

Service providers and any third party involved in age assurance should ensure that the processing of any personal data for the purposes of age assurance is lawful, fair and transparent to users.

23. Service providers must ensure that they have an applicable legal basis under Article 6 GDPR (and, if relevant, applicable exception laid down in Article 9(2)) to process personal data in the context of age assurance. For example, they may need to deploy age assurance in order to comply with a legal obligation (Article 6(1)(c) GDPR), taking into account that age assurance must be proportionate to the legitimate objective pursued and the requirements set out in Article 6(3) GDPR.

24. Furthermore, service providers must be transparent with users about how exactly their personal data is being used and by whom. This is particularly important when there are multiple parties involved in the age assurance process. Before any personal data is processed for the purposes of age assurance, users must be informed (pursuant to Articles 12, 13 and 14 GDPR), amongst other things, about[25]:

- what personal data will be processed and how;
- whether third parties will be involved in the process, and if so, who they are and who the controllers and processors are in this scenario;
- if their data will be shared with others or transferred to a third country;
- how long their personal data is going to be retained or, if this is not possible, the criteria to determine the storage period;
- what their rights are in relation to their personal data (Articles 15 to 22 GDPR), including how they can challenge an incorrect decision made as a result of age assurance.

25. Transparency in the context of age assurance is particularly important when it comes to children. Service providers must ensure that they convey transparency information to children, when concerned, in a way that is clear and easy for them to understand.

26. The concept of transparency is fundamentally linked to fairness. If service providers are not clear and transparent about how they are processing natural persons' information for age assurance, then it is unlikely that this processing can be considered fair, which in turn makes it unlikely that this processing is lawful. In particular, if a provider offers different methods for users to verify their age, they should be transparent about the impact that each method has from a data protection perspective.

[25] See the Article 29 Working Party Guidelines on transparency under Regulation 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf

2.7 Automated decision-making

Any occurrence of automated decision-making in the context of age assurance should comply with the GDPR. If applicable, service providers and any third party involved should provide suitable measures to safeguard natural persons' rights and freedoms and legitimate interests.

27. The EU legislator has opted for a broad definition of automated decision-making that requires examination on a case-by-case basis[26]. Automated decisions can be involved at different stages in the age assurance process, either for accessing the content or service, or through the methods deployed to prove age.

28. Fully automated age assurance can produce legal effects on the natural persons concerned – for example on the exercise of their freedom of expression – or, at the very least, can significantly affect them in a similar way[27]. The effect of automated age assurance on natural persons' rights can vary according to the type of content or services involved.

29. Therefore, service providers and any third party involved in age assurance should provide remedies and appropriate redress mechanisms for users whose age-related attributes are not properly established. Depending on the architecture of the age assurance process, they must identify who the data subject should contact to exercise their rights[28].

30. Service providers and any third party involved should pay particular attention when children are concerned. As stated in Recital 71 of the GDPR, *'solely automated decision-making […] with legal or similarly significant effects […] should not concern a child'*. Exceptions to this rule should remain under limited circumstances, such as where it is necessary *'to protect their welfare'*[29]. In any case, service providers and any third party involved should implement suitable measures – e.g. viable alternatives, redress mechanisms, and, where applicable, human intervention – with information adapted for children, when concerned.

2.8 Data protection by design and by default

Age assurance should be designed, implemented and evaluated taking into account the most privacy-preserving available methods and technologies in order to meet the requirements of the GDPR and effectively protect the rights of data subjects.

31. Under Article 25 GDPR, data controllers involved in age assurance should implement appropriate technical and organisational measures and necessary safeguards to provide effective implementation of all data protection principles and, consequentially, data subjects'

[26] Case C-634/21, SCHUFA Holding (Scoring): Judgment of the Court (First Chamber) of 7 December 2023 (request for a preliminary ruling from the Verwaltungsgericht Wiesbaden — Germany) — OQ v Land Hessen (Reference for a preliminary ruling — Protection of natural persons with regard to the processing of personal data — Regulation (EU) 2016/679 — Article 22 — Automated individual decision-making — Credit information agencies — Automated establishment of a probability value concerning the ability of a person to meet payment commitments in the future ('scoring') — Use of that probability value by third parties), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62021CA0634

[27] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/items/612053/en

[28] As stated in the EDPB guidelines (above-mentioned): '*these rights are actionable against the controller creating the profile and the controller making an automated decision about a data subject (with or without human intervention), if these entities are not the same*'.

[29] From the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679: '*There may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children, for example to protect their welfare'.*

rights and freedoms. The requirement for controllers to have data protection taken into account by default at design stage of any processing activity of personal data also applies to processors and throughout a processing lifecycle.

32. Considering the diversity and severity of the risks associated with age assurance systems, especially when identity documents or special categories of personal data such as biometric data are processed, the utmost attention should be paid to avoid any unnecessary access to, processing, sharing and storage of personal data. Age assurance systems and any legal or technical instrument setting out requirements for such systems should also be regularly revised and updated, if necessary, to take into account the quickly moving landscape of privacy enhancing technologies in the field of digital identity management.

33. As mentioned in the EDPB guidelines on data protection by design and by default[30], the reference to "state of the art" in the context of Article 25 GDPR imposes an obligation on data controllers to consider the current progress in technology that is available in the market when determining the aforementioned appropriate technical and organisational measures. Standards, best practices and codes of conduct that are recognised by relevant stakeholders can be helpful in determining such measures. However, the appropriateness of these measures should be verified for each particular processing activity.

34. Consequentially, the EDPB recommends that, based on the state of the art in age assurance at the time this document was prepared, due consideration is given to technologies and architectures favouring user-held data and secure local processing (device-based), allowing properties such as unlinkability[31] (from different parties' point of view and even in the case of collusions or data breaches) and selective disclosure[32] of personal data under the control of the data subject. In addition, the use of approaches such as those relying on batch issuance[33] of single-use credentials or cryptographic protocols such as zero-knowledge proofs[34] should be made available for the data subjects in cases where age assurance may involve high risks to their privacy.

2.9 Security of age assurance

Service providers and any third party involved in age assurance should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

35. The GDPR requires both controllers and processors to have appropriate technical and organisational measures in place to ensure a level of security appropriate to the risk posed to the personal data being processed (Recital 83 and Article 32). The nature, sensitivity, and

[30] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[31] The unlikability property implies that it is impossible to associate or correlate different data items, actions or transactions to a specific data subject.

[32] Selective disclosure is a feature of tokens, credentials and attestations that allows data subjects to share only the information they want with specific parties on a case-by-case basis.

[33] Batch issuance relies on responding to one credential request from the data subject with a set or group of credentials produced at the same time.

[34] A zero-knowledge proof is a protocol in which one party (the prover) can demonstrate another party (the verifier) that some given statement is true, without conveying to the verifier any information beyond the mere fact of that statement's truth.

volume of personal data that can be involved in age assurance highlight the potential adverse effect that a data breach could entail.

36. Trust models are crucial to prevent data breaches in age assurance contexts, as they define how the different parties can verify each other's identities and integrity. They facilitate secure communication and data exchange among participants who may not have prior relationships. In addition, pseudonymisation and encryption of personal data may be helpful measures to mitigate the possible adverse effects of data breaches. Fulfilling the storage limitation principle and using short retention periods may also be essential for security in age assurance, reducing the exposure surface. A no-log policy may be considered a valuable safeguard: once the user's age is verified, no record of the personal data used for the age assurance process is kept.

37. In practice, given the increasing legal pressure to implement age assurance and the number of providers that may be subject to such rules, the occurrence of security breaches should be expected. It should be ascertained whether all appropriate technological protection and organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[35]. A key element of any data security policy is being able, where possible, to prevent a breach and, where it occurs, to react in a timely manner. Therefore, the ability to promptly restore the availability of age assurance after a security breach should also be considered as essential. Similarly, it is crucial to ensure the resilience of the age assurance ecosystem, favouring the existence of different alternatives and loosely coupled parties[36] that do not depend so much on each other that the failure or breakdown of one would cause significant access limitations.

38. While security measures are of the utmost importance in age assurance, they do not guarantee that authorised or unauthorised access to personal data will not impact the rights of natural persons. They cannot replace the application of the principles of necessity, proportionality or data protection by design and by default.

2.10 Accountability

Service providers and any third party involved should implement governance methods that allow them to be accountable for their approach to age assurance and for demonstrating their compliance with data protection regulation and other legal requirements.

39. Given the involvement of different stakeholders, age assurance governance plays a crucial role in its accountability. Age assurance should operate under a governance framework, ensuring that all processes and systems are designed, implemented, revised, documented, assessed, used, maintained, tested or audited in a way that meets data protection regulations and other legal requirements. This framework should include, at least, the data protection policies (Article 24(2) GDPR) and the prioritisation and decision-making processes required to

[35] From the EDPB Guidelines 9/2022 on personal data breach notification under GDPR, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

[36] Parties depend on each other to the least extent possible, reducing the scope of impact when changes or failures occur.

achieve compliance objectives and to manage the risks appropriately over the entire age assurance lifecycle.

40. For example, the governance framework should delineate who is responsible and how, from a controller/processor perspective, for which exact activities or operations within the processing. It should also ensure that age assurance is effectively auditable by authorities and relevant stakeholders. The governance framework is essential for accountability, but also for transparency and trust in age assurance. Data subjects are more likely to trust methods that are transparent about their operations, decision-making, etc.

41. Furthermore, part of the governance framework involves ensuring effectiveness (section 2.5), data protection by design and by default (section 2.8), and security (section 2.9) of age assurance.

For the European Data Protection Board

The Chair

(Anu Talus)