G7 DATA PROTECTION AND PRIVACY AUTHORITIES ROUNDTABLE

STATEMENT FOR PRIVACY-PRESERVING AGE ASSURANCE

1. Following the adoption of the G7 Data Protection and Privacy Authorities' Action Plan in June 2025 [1], and the commitment to "remain attentive to the impact that emerging technologies can have on privacy, particularly on children's privacy" we, the G7 Data Protection and Privacy Authorities (G7 DPAs), met to discuss the recent developments and challenges raised by the deployment of age assurance solutions from a data protection and privacy perspective.

2. We note that G7 jurisdictions' respective regulatory frameworks or strategies endeavour to enhance the protection of children in the digital environment. Operationalizing this protection can include encouraging the use of age assurance by online service providers where appropriate. This may include, for example, situations where risks to children cannot be mitigated as effectively by other less intrusive means, or, where national laws prescribe a minimum age to use a service (such as social media) or prohibit children from accessing certain types of content (e.g., pornographic content).

3. In this regard, we take note of the G7 Ministerial Declaration on Digital & Technology adopted on May 29,2026 in Paris and of the G7 Common Set of Principles defining a safer and more secure digital space for minors which states that "effective age assurance is key to ensure a safer, more secure, and age-appropriate experience for minors", and welcome the commitment made by the G7 Digital & Technology Ministers to rely on "robust, reliable, risk-based, appropriate, rights-respecting, privacy-preserving and interoperable age assurance solutions".

4. While age assurance can be useful, we recognize that it is only one of the available tools that can contribute to the protection of children in the digital environment. Parental control systems and, more generally, digital literacy initiatives for both children and responsible adults are also important to protect children online. We highlight that age assurance online should be used with appropriate privacy protection and limited to specific contexts. This is because the indiscriminate use of age assurance technologies could pose significant risks to individuals' rights and freedoms.

5. We recognize that age assurance technologies are evolving to help address the challenges of protecting children in a digital environment, and we support the focus on interoperability, trustworthiness, and privacy within the development process.

6. We welcome the efforts already made by some Data Protection and Privacy Authorities to provide guidance for the deployment of age assurance tools in a privacy-protective manner, and take

[1] G7 Data Protection and Privacy Authorities' Action Plan in June 2025

note of the following publications: The Joint Statement on a Common International Approach to Age Assurance[2], the EDPB Statement on Age Assurance[3], the FTC COPPA Policy Statement [4], and OPC Canada Age Assurance Guidance [5]. We also take note of international efforts like the ISO 27566 framework[6] which establishes a framework for age assurance systems.

7. We draw attention to the following key data protection and privacy issues raised by age assurance technologies, including but not limited to:

a. **Protection of rights and freedoms**: Age assurance measures should comply with individuals' rights and freedoms consistent with applicable legal frameworks, such as the right to free expression and to access information, and in particular paying attention to children's interests, safety and well-being online to the fullest extent.

b. **Prevention of privacy risks and purpose limitation**: Age assurance measures should avoid creating unnecessary risks to individuals' privacy, including when third parties are involved, and should not be used to enable the identification, tracking, profiling, or monitoring of individuals. Similarly, the result of the age assurance process should not be used for any other purpose than the one that made the age assurance necessary.

c. **Collection, use and retention limitation:** The collection, use and retention of information needed to determine a user's age should be limited to what is necessary to achieve the specific purpose of age assurance, in compliance with applicable legal frameworks.

d. **Effectiveness:** Age assurance measures should be effective (e.g., with regard to accessibility, reliability and robustness) in fulfilling their intended purpose, relying on approaches that are accurate and proportionate to the context.

e. **Lawfulness, fairness and transparency:** Online service providers and any third parties involved in age assurance should handle personal data in a manner that is consistent with applicable legal requirements, and provide clear and understandable information in its notice to users, including children.

f. **Privacy by design:** Considering privacy at the design, implementation and operation phases of age assurance can help to ensure that individuals' privacy is protected in line with the state of the art, and may be required in some juridictions. This includes evaluating the effectiveness of protections regularly.

[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/joint-statement-on-a-common-international-approach-to-age-assurance/introduction/
[3] https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf
[4] FTC Issues COPPA Policy Statement to Incentivize the Use of Age Verification Technologies to Protect Children Online | Federal Trade Commission
[5] News release: Privacy Commissioner of Canada launches new age assurance guidance to support organizations - Office of the Privacy Commissioner of Canada
[6] ISO/IEC 27566-1:2025 - Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework

g. **Security:** Online service providers and any third parties involved in age assurance should implement reasonable and appropriate technical and organizational measures to ensure the security of personal data, considering the sensitivity of the information and the level of risk involved.

8. We agree to continue to exchange information on personal data and privacy protection in the context of age assurance within the G7 Data Protection and Privacy Authorities Roundtable, and to explore how to contribute to discussions in other international fora in order to promote these key issues and privacy principles regarding age assurance. We also commit to continue our engagement with other competent regulators, including in the media and online safety fields, to promote applicable privacy-preserving principles when using age assurance.