

G7 DATA PROTECTION AND PRIVACY AUTHORITIES ROUNDTABLE

COMMUNIQUÉ

25-26 JUNE 2026

1. We, the data protection and privacy authorities of the G7 member countries, met on 25 and 26 June 2026 under the presidency of the Commission nationale de l'informatique et des libertés (CNIL) in Paris, France, to discuss emerging technological developments, data protection and privacy, and opportunities for international cooperation in support of a trusted digital environment across borders.
2. We welcomed the Executive Committee of the Global Privacy Assembly (GPA) represented by its Chair, the Privacy Commissioner of Canada, the Global Privacy Enforcement Network (GPEN) represented by the United States Federal Trade Commission, the Governance Committee of the Asia Pacific Privacy Authorities (APPA) Forum represented by the Personal Data Protection Commission (PDPC) of Singapore, the Association francophone des autorités de protection des données personnelles (AFAPDP) represented by the Data Protection Commissioner of Mauritius, and the Personal Information Protection Commission (PIPC) of Korea to enhance the global perspective in our discussions and to strengthen cooperation between different networks of data protection and privacy authorities.
3. We also welcomed representatives of the Committee of Convention 108 of the Council of Europe, represented by the Agencia Nacional de Acceso a la Información Pública (AAIP) of Argentina, and of the Organization for Economic Co-operation and Development (OECD).
4. During our meeting, we discussed several key issues with a view to share our expertise, experience and explore possible cooperation:
 - a. **Children's protection online and age assurance.**
 - i. G7 jurisdictions' respective regulatory frameworks or strategies endeavour to protect children in the digital environment. Operationalizing this protection can include encouraging the use of privacy-preserving age assurance by online service providers. In that regard, we 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" and draw attention to key data protection and privacy principles in our Statement for privacy-preserving age assurance with the aim of protecting children online while also respecting the protection of personal data and privacy.
 - ii. We also discussed the fact that, numerous applications and software programs based on artificial intelligence (AI) now allow users to easily create increasingly sophisticated deepfakes, resulting in their online proliferation, along with the associated risks of personal data's misuse, particularly the

creation of intimate imagery without individuals' consent, notably children. We take note of the efforts made by some data protection and privacy authorities to take enforcement actions and to remind developers, deployers, and users of such AI systems of the need to respect applicable legal frameworks, including data protection and privacy laws, and of taking measures to prevent the generation of such content. We also take note of the efforts made by some data protection and privacy authorities to encourage parents to limit sharing photos or videos of their children on social networks, especially if their profile is public.

b. **Connected Home Devices and Children's Privacy.** We highlight the work conducted under the leadership of the UK's Information Commissioner's Office (ICO) in developing a paper on Connected Home Devices and Children's Privacy. The paper identifies key considerations for responsible data practices for connected home devices that are targeted at children, process children's information or are likely to be used by children. We will continue in our collaborative efforts to identify new technologies which may pose challenges for data protection and privacy, and to share our expertise in discussing topics of mutual interest.

c. **Smart glasses.** We take note of the efforts of the CNIL's presidency in supporting our discussion by presenting its Compendium of data protection and privacy authorities approaches on smart glasses. On the basis of this document of the G7 DPAs' presidency, we discussed the benefits that smart glasses can provide to individuals as well as privacy risks, ethical and societal issues they can raise, including the collection and use of substantial volumes of personal data, the covert collection of individuals' images and voices without their knowledge and a heightened risk of general surveillance in public and private space. We will strengthen our cooperation and knowledge sharing on this issue.

d. **Agentic AI.** We discussed the capabilities of agentic AI systems, the opportunities they afford, and the potential challenges agentic AI systems may raise in relation to data protection and privacy, including the significant autonomy of Agentic AI systems, the increasing complexity of the supply chain, the automated decision-making and the reduction of human intervention. We will continue to share information to improve our collective knowledge of these systems.

e. **Enforcement cooperation.** With a view to fostering enforcement cooperation between data protection and privacy authorities, we value our ongoing dialogue within the G7 Data Protection and Privacy Authorities Roundtable and we welcome all efforts to facilitate information sharing where possible. In this regard, we welcome the efforts made by the Personal Information Protection Commission of Japan (PPC) to put in place a repository of G7 Data Protection and Privacy Authorities public enforcement cases.

f. **Data Free Flow with Trust.** We welcome the G7 Digital & Technology Ministers' reiteration of "the importance of maintaining trust-based data frameworks based on [their] commitment to Data Free Flow with Trust (DFFT), respecting applicable legislation on privacy, data protection, intellectual property rights, including trade secrets, and security, while preserving governments' ability to address legitimate public policy objectives". We will continue our dialogue on the infrastructure for cross-border data transfer in our respective jurisdictions, including provisions regarding government access to personal data, to work towards even more commonalities, complementarities and elements of convergence between our respective regulatory approaches and transfer tools in order to foster their future interoperability and facilitate trusted cross-border data flows.

5. We remain committed to ongoing cooperation to support a trusted digital environment and promote responsible innovation. We look forward to our next meeting under the presidency of the United States in 2027.