

## **G7 DPAs' Action Plan**

We, the G7 Data Protection and Privacy Authorities (DPAs), endorse the following Action Plan on the three pillars set out by the 2023 Communiqué, namely (I) Data Free Flow with Trust (DFFT), (II) Emerging technologies, and (III) Enforcement cooperation. In doing so, we commit to:

### **Pillar I - DFFT**

#### **Developing DFFT**

1. Remain attentive and supportive to the ongoing efforts to develop the concept of DFFT, as progressed within several international fora such as our G7 working group, the Global Privacy Assembly (GPA), the Organization for Economic Co-operation and Development (OECD), including through the announcement of the creation of a new Institutional Arrangement for Partnership (IAP), and emphasize that trust is a vital component to the flow of data on a global scale.
2. Reach a common understanding of the notion and key components of DFFT as far as personal data is concerned and assess common goals to ensure a high level of data protection and privacy.

#### **Transfer tools**

3. Build on the conclusions of the G7 DPA Roundtable in Bonn in 2022 which recognized data transfer tools as important means for DFFT.
4. Continue working towards elements of convergence to foster future interoperability of these transfer tools, where possible, and identify specific use-cases for their interoperable use, in order to achieve a high level of data protection and facilitate DFFT.
5. Contribute to and support the work that is being undertaken by the Global Frameworks and Standards Working Group of the GPA, through the existing membership of the G7 DPAs.
6. Share knowledge on tools for secure and trustworthy transfers, notably through the comparison of Global Cross-Border Privacy Rules (CBPR) and EU certification requirements, and through the comparison of existing model

contractual clauses. This work will assess the level of interoperability and convergence between different certification mechanisms and other tools for transfers, and map commonalities and possible differences as well as areas for further improvement.

7. Identify opportunities for longer term initiatives for the DFFT Working Group, including progressing discussions on how DPAs can play an active role in the development of the IAP.

### **Government access to data**

8. Commend the 2021 GPA resolution on Government Access to Data, Privacy and the Rule of Law.
9. Encourage the OECD to continue its work on trusted government access including considering further steps to promote and develop approaches in support of its Declaration on Government Access to Personal Data held by Private Sector Entities adopted at the OECD Ministerial meeting in December 2022.
10. Considering its universal nature, encourage non-OECD members to refer to the OECD Declaration and reflect it in their policy making.

### **Pillar II - Emerging technologies**

11. Seek to promote the development and usage of emerging technologies in ways that reinforce trust and respect privacy.

### **Terminology reference document**

12. Facilitate collaborative work and discussions on de-identification, anonymization, pseudonymization, and Privacy-Enhancing Technologies (PETs) by fostering a common understanding of key terms and concepts in use across G7 jurisdictions.
13. Develop a terminology reference document outlining key terms and characteristics relating to de-identification, anonymization, pseudonymization,

and PETs in use among G7 DPAs to facilitate collaborative work and discussions.

- The document will note how terms are defined, explain common features across jurisdictions, and note important differences between jurisdictions. It will also address relevant international definitions/uses of terms (e.g. International Organization for Standardization (ISO) standards), and will contain references to sources of information, guidance, and definitions for key terms in G7 jurisdictions.

### **PETs use case study**

14. Encourage the adoption and development of PETs by developing a use case demonstrating how one specific PET (synthetic data) can be used to reduce privacy risks while contributing to the public benefit.
15. Bring regulatory insights to this emerging market and encourage the use of such technologies, by demonstrating, through this use case, how synthetic data can be used for the purpose of sharing health data to help achieve a safe and privacy-enhancing method for obtaining insights from sensitive data.
  - The use case will seek to explain how generating local-level synthetic datasets of prescriptions can allow insights to be gained at a wider geographic level without the need to share sensitive information about individual prescriptions and provide information about how such a process can take place, what technical and organizational measures are required and what privacy considerations are relevant.
16. Share knowledge and existing work in this area and identify opportunities to engage with subject matter experts and other relevant stakeholders.
17. Discuss how to proceed with other PETs in this Working Group without limitation to use case studies once the analysis of one type of PET (synthetic data) is completed.

## **Support for GPA resolution on principles for the use of facial recognition technology**

18. Welcome the GPA 2022 Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology (FRT), which seeks to establish a set of shared principles for FRT use by public and private organizations around the world.
19. Promote these principles and expectations to stakeholders worldwide, by:
  - Citing and hyperlinking the text of the principles and expectations, where relevant and appropriate, in documentation on AI and FRT-related topics produced by Emerging Technologies Working Group members;
  - Encouraging support for the principles and expectations, as and where appropriate, among external stakeholder groups.
  - Advocating for safeguards that are consistent with the principles and expectations, as and where appropriate in members' jurisdictions.

## **Collaboration on personal data protection in the context of generative AI**

20. Collaborate on the issue of personal data protection within the context of generative AI from an ethical, legal, social, and technical perspective.
21. Contribute to discussions on generative AI in other international fora, while emphasizing the need to pay close attention to data protection and privacy issues.
22. Explore how best to protect privacy in relation to generative AI.

## **Pillar III- Enforcement cooperation**

### **Increasing Enforcement Dialogues amongst G7 DPAs and the broader data protection and privacy enforcement community**

23. Foster greater dialogue, through the G7 Enforcement Cooperation Working Group and with the broader privacy enforcement community, in relation to enforcement cooperation matters, including enforcement of laws and regulations, to ensure a high level of data protection and privacy, and to identify and overcome legal and practical challenges for cross-border enforcement cooperation.
24. Seek out, advocate for, and actively participate in discussions on these topics at existing fora such as the GPA's International Enforcement Cooperation Working Group (IEWG), the Global Privacy Enforcement Network (GPEN) and others.
25. Share both domestic and international best practices for effective enforcement collaboration, including successful cooperation cases.
26. Discuss ways to promote implementation of data minimalization principles and efforts to disseminate these principles worldwide, and share lessons learned and examples of remedies to achieve data minimization.
27. Explore differences in enforcement from perspectives of deterrence, accountability, and protection of individuals.

### **Interventions by the G7 Enforcement Cooperation Working Group to Support Existing Enforcement Cooperation Activities**

28. Establish a G7 DPA Contact List to promote ongoing information sharing and encourage GPEN to expand and refresh its own contact list, by notably incorporating the G7 Contact List.
29. Build on the influence of the G7 DPAs to promote agile and efficient cooperation, including by (i) enhancing the established G7 DPA Request for Information (RFI) format at G7 Enforcement Cooperation Working Group, (ii) considering to work towards establishing a new bilateral Memorandum of Understanding (MoU) or Memorandum of Cooperation (MoC) amongst G7 DPAs, and (iii) incorporating the RFI format and the existing MoUs and MoCs into the GPA's Enforcement Cooperation Handbook, to serve as examples for other DPAs.

30. Lead by example, by seeking out opportunities to engage in concrete bilateral or multi-lateral enforcement cooperation amongst G7 member authorities, and by sharing information and/or undertaking joint or coordinated enforcement actions in relation to data protection and privacy issues of global significance.

### **General Support and Amplification of Existing Enforcement Cooperation Activities**

31. Support and encourage the global DPA community to engage with global and regional fora to leverage the various tools and mechanisms for enforcement cooperation made available by those networks to expand our collective enforcement capacity and create the foundation for successful cooperation. To this end, the G7 Enforcement Cooperation Working Group undertakes the following.
32. Encourages participation in the GPA, including:
  - the Global Cross Border Enforcement Cooperation Arrangement of the GPA (“Mauritius Arrangement”)
  - the GPA’s IEWG, in respect of which we welcome the efforts to update the Enforcement Cooperation Handbook and Repository; and
  - the Digital Citizen and Consumer Working Group of the GPA which promotes cross-regulatory dialogues and practical cooperation where privacy intersects with other regulatory spheres (e.g., Competition).
33. Encourages participation in GPEN and its various tools and initiatives, such as Privacy Sweeps, capacity building webinars and online discussion forum, and supports the implementation of its updated Action Plan.
34. Welcomes the OECD’s ongoing work to review its Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy and encourages the OECD to work with enforcement fora including the G7, GPA, and GPEN to assess overlaps, commonalities, complementarities, and opportunities for coordination across the existing frameworks and networks for enforcement cooperation.
35. Takes note of the developments in regional networks to foster global enforcement cooperation amongst DPAs, including:

- a) the European Data Protection Board's (EDPB's) toolbox on essential data protection safeguards for enforcement cooperation between EEA and other DPAs; and
- b) the ongoing work of the Global Cooperation Arrangement for Privacy Enforcement (CAPE), which would underpin the coming CBPR System.

## **Working groups and evaluation**

- 36. Continue dialogues amongst G7 DPAs at the DFFT, Emerging Technologies and Enforcement Cooperation Working Groups.
- 37. Evaluate the progress and achievements of this action plan at the 2024 G7 DPA Roundtable to be held in Italy.