Roundtable of G7 Data Protection and Privacy Authorities

– Communiqué –

8 September 2022

Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces

1. We, the data protection and privacy authorities of the G7 member countries, met on 7 and 8 September 2022 under the chairpersonship of the German Federal Commissioner for Data Protection and Freedom of Information, Professor Ulrich Kelber, to discuss current regulatory and technology issues and developments in the context of "Data Free Flow with Trust (DFFT)" and share knowledge about the prospects for "international data spaces", which can be seen as an emerging approach to trusted and voluntary data sharing within and across organisations and sectors, whether domestically or internationally, to support innovation in academia, industry and the public sector. The meeting took place within the framework of the Digital Ministers' G7 Digital Track of the German G7 Presidency in 2022.

2. We welcome the commitment by the G7 Digital Ministers in the Ministerial Declaration of 11 May 2022 to "maintain a free, global, open, interoperable, reliable and secure Internet that supports innovation and strengthens respect for democratic values and universal human rights" and to shape digital transformation in line with our liberal democracies. We also appreciate the commitment by the G7 Leaders in the Leaders' Communiqué of 28 June 2022 to strengthen their efforts "to facilitate DFFT across borders, continue to harness opportunities, and to address challenges raised, in particular in relation to security, privacy and data protection".

3. The importance of democratic principles and fundamental human rights in the digital world has recently been underlined by the European Union, the United States of America and many other nations, including all G7 members, in the "Declaration

for the Future of the Internet". We, as G7 data protection and privacy authorities, regard the principles of democracy, rule of law and fundamental rights, including the rights to privacy and data protection, as guiding principles also with respect to the concept and further development of DFFT.

4. Adherence to democratic values and fundamental human rights of individuals is likewise an obligation for public authorities and the corporate sector. With regard to human rights this is underlined in the United Nations' 2011 Guiding Principles on Business and Human Rights. Where entities infringe the law by processing personal data based on intrusive and hidden methods to track and monitor private behaviour of individuals or consumers across apps, websites, and devices, it is incumbent on data protection and privacy authorities to enforce the law in an effective, proportionate, compliance-enhancing and independent manner.

5. Further, the regulatory spheres of privacy, competition and consumer protection continue to intersect. Enforcement by competition authorities is becoming increasingly relevant where abusive behaviour with respect to personal data is carried out by dominant companies or data-driven companies exercising significant market power across industries. We welcome efforts by data protection and privacy, competition and consumer authorities to cooperate across borders and regulatory spheres and we call on G7 countries to further strengthen their efforts to advance meaningful cross-regulatory collaboration, holistically protecting privacy rights while supporting a robust digital economy. The G7 data protection and privacy authorities (DPAs) highlight the work of the Global Privacy Assembly (GPA), which all G7 DPAs are a member of, and the OECD in advocating for such cross-regulatory collaboration.

6. We welcome the continuation of the UK 2021 G7 Roadmap for Cooperation on DFFT under the 2022 German G7 Presidency. The G7 Action Plan for Promoting DFFT, adopted by the Digital Ministers on 11 May 2022, foresees important actions and initiatives with relevance to trustworthy international data flows, including the need for identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments such as standard contractual clauses in order to foster future interoperability.

7. With respect to transfer instruments, we recognize the importance of discussions about several current approaches in different regions of the world, which should be inclusive and not exclusive. We therefore commit to continue working towards elements of convergence of these tools to foster future interoperability, where possible, in order to achieve a high level of data protection and facilitate data free flow with trust and create options for businesses to choose cross-border transfer tools, suitable for their business needs. In that regard, we support the ongoing work undertaken by the Global Frameworks and Standards Working Group of the GPA and by the OECD on the comparison of cross-border transfer mechanisms and commit to exchange our experience and best practices in this regard, both, within the GPA and amongst G7 DPAs.

8. We recognize adequacy decisions among G7 member countries as a tool to enable free and trustworthy flows of personal data with high data protection standards and we encourage the US government and the European Commission to intensify their efforts for a new, solid Trans-Atlantic Data Privacy Framework.

9. We as data protection and privacy authorities of the G7 member countries call upon governments to continue efforts to implement effective data protection and privacy laws and to build upon existing frameworks and approaches, such as the Convention 108+ of the Council of Europe, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.

10. In this context[1], we commend the 2021 GPA Resolution on Government Access to Data, Privacy and the Rule of Law and welcome the commitment by the G7 Digital Ministers to further support work being done by the OECD on the same sensitive topic. As stated in the Resolution, we underline that to effectively protect the fundamental rights to data protection and to privacy, clear and precise rules governing the scope and the conditions under which privately held data might be accessed for national security and public safety purposes need to be laid down by appropriately enacted legislation which ensures that interferences are limited to what is strictly necessary and proportionate in democratic societies. In our view, it is vital to consider and to explore how democratic principles and legal restrictions on government access can also be guaranteed in the context of DFFT at international level by multilateral instruments ensuring adherence to key data protection and privacy principles.

11. In addition to regulatory issues, we also discussed technological aspects required of safeguarding international transfers. A particular focus amongst the G7 should be on privacy enhancing technologies (PETs).

12. Considering the importance of the work of data protection and privacy authorities on data related issues at international level, we strongly encourage G7 governments to consult the expertise of their data protection and privacy authorities in data-related work in international organizations and fora at an early stage on a regular basis. We therefore welcome the commitment made by the G7 Digital Ministers to promote regulatory cooperation for DFFT “including through the continuation of dialogue among G7 policy officials and Data Supervisory Authorities and/or other competent authorities for data”.

[1] This paragraph relates to matters outside the jurisdiction of the U.S. Federal Trade Commission.

13. For the practical implementation of this regulatory cooperation, the G7 data protection and privacy authorities agreed to establish the Data Protection and Privacy Roundtable meetings as a permanent grouping with annual meetings at Commissioner's level and continued exchange at expert level. The Roundtable should complement the work of other international fora and leverage the weight of G7 members to amplify the voice of other networks. We also encourage G7 governments to ensure that the dialogue between policy makers and regulators becomes an integral part of the G7 digital agenda, when data and privacy related issues are at stake.

14. At this roundtable, we have continued to reflect on topics developed at the 2021 UK G7 Roundtable. Involving subject matter experts from our organisations, we held meetings at working level in the first half of 2022 to review the developments in artificial intelligence (AI), online tracking, pandemic driven technological innovation, cross-border enforcement cooperation, cross-regulatory intersections, redesigning remedies and government access to data. Building on the results of each Working Group, we recognise the necessity of further discussion on important issues and will continue an engagement at working level of the G7 data protection and privacy authorities. A summary of these discussions is in the Annex to this Communiqué.

15. We have also started to widen our discussions on further topics relevant to DFFT and to share knowledge about the prospect for international data spaces. These topics are: international data transfer tools including certification mechanisms, privacy enhancing technologies, de-identification standards and the place for de-identified data in data protection and privacy law, the principles of data minimization and purpose and use limitations in the context of commercial surveillance and opportunities and the role of data protection and privacy authorities in setting and promoting an ethical and cultural model for AI governance. International data transfer tools, including among others certification, and methods of de-identifying data can complement each other to facilitate data flow while ensuring continuity of protection. This demonstrates the cohesion amongst the G7 DPAs on these vital topics. Building on the results of the discussions, we will continue to discuss developments in the context of DFFT. A state of play of these discussions is in the Annex to this Communiqué.

16. We note the appreciation in the G7 Digital Ministers of the intention of the Japanese G7 Presidency in 2023 to continue work promoting regulatory cooperation for DFFT "in particular through roundtable discussions of data protection and privacy authorities". In this context, we will continue our engagement at expert level with the aim of developing an Action Plan and preparing the Roundtable meeting under the chairpersonship of the Personal Information Protection Commission (PPC), Japan, in 2023.

ANNEX – SUMMARY OF TOPICS DISCUSSED

Follow-up from the G7 DPA Roundtable and Communiqué 2021

Technologies Working Group

17. The Technologies Working Group, hosted by the Information Commissioner (ICO), UK, discussed updates to the technology focused provocations on 'Artificial Intelligence', 'Pandemic Driven Tech Innovation' and 'Shaping the Future of Online Tracking'. Each DPA provided an update on the work that had been undertaken since September 2021, and discussion considered how some of this work could be progressed further. G7 DPAs agreed that the working group should continue to meet regularly.

Enforcement Cooperation Working Group

18. The Enforcement Working Group, hosted by the PPC, Japan, discussed several regulatory issues, in particular enforcement cooperation, privacy and competition intersection, redesigning remedies, and government access, and shared information on activities in other international fora such as the OECD, the GPA, and GPEN (Global Privacy Enforcement Network), as well as on best practices such as joint investigation and operationalization of Memoranda of Understanding.

19. Participants pointed out the necessity and importance of effective information exchange amongst G7 DPAs, enhancing cooperation with competition and consumer protection authorities, developing each national legal systems for deterrent measures, and supporting ongoing work in other international organizations on government access.

20. We will continue engagement at working level to develop tangible outcomes on common important issues, and consider how we add a value to them as the G7 data protection and privacy authorities towards 2023.

2022 Topics discussed in the context of Data Free Flow with Trust (DFFT) and international data spaces

International data transfer tools including certification

Prepared by CNIL, BfDI and PPC

21. The G7 data protection and privacy authorities underline that in the absence of agreed multilateral rules governing regulatory aspects of cross-border data flows, data transfer tools are important means for DFFT and may also contribute to the sharing of knowledge about the prospects for international data spaces and to facilitate elements of convergence to foster future interoperability, where possible, between different national and regional data protection and privacy frameworks.

22. We acknowledge the worldwide progress made in this area, e.g. in the EU by the recent adoption of EDPB Guidelines on Certification and Code of Conducts as tools for transfers or by the new Standard Contractual Clauses issued by the European Commission in 2021, in Asia e.g. by the adoption of ASEAN Model Contract Clauses, in Latin America, e.g. by issuing model contractual clauses of the Ibero-American Data Protection Network (RIPD), or in the Asian-Pacific Area, e.g. by the Global CBPR Forum initiative as an evolvement of the APEC CBPR system.

23. We commit to continue working towards elements of convergence to foster future interoperability of these transfer tools, where possible, in order to achieve a high level of data protection and facilitate data free flow with trust. In that regard, we support the ongoing work undertaken by the Global Frameworks and Standards Working Group of the GPA and the OECD on the comparison of cross-border transfer mechanisms and commit to exchange our experience and best practices in this regard, both, within the GPA and amongst G7 DPAs. We recognize the importance of creating an environment where businesses can choose cross-border transfer tools, based on their business needs and their obligation to protect individuals' rights. We also encourage lawmakers and other stakeholders to support the development of these tools and to analyze differences in the level of protection and the regulatory approaches with the aim of promoting elements of convergence to foster future interoperability of them, where possible, and bridging differences, including availability of enforceable data subject rights and effective legal remedies for data subjects and consumers in different jurisdictions.

Privacy Enhancing Technologies

Prepared by ICO

24. The April 2021 Ministerial Declaration of the G7 Digital and Technology Ministers highlighted the importance of unlocking the power of data in G7 economies and societies, while continuing to address challenges related to privacy, data protection, intellectual property rights, and security.

25. Privacy-enhancing technologies (PETs) – such as trusted research environments, federated learning, differential privacy, zero knowledge proofs, secure multiparty computation and homomorphic encryption – help organizations implement or improve data protection by design through processes which mask or transform personal data to reduce its identifiability.

26. The use of PETs can facilitate safe, lawful and economically valuable data sharing that may otherwise not be possible, unlocking significant benefits to innovators, governments and the wider public. In recognition of these benefits we, as the G7 data protection and privacy authorities, will seek to promote the responsible and innovative use of PETs to facilitate data sharing, supported by appropriate technical and organizational measures.

27. In tandem with taking action ourselves to support organizations to use PETs in compliance with data protection and privacy law, we call on industry to develop the technical standards and certification schemes needed to give organizations confidence that they are using PETs responsibly and in compliance with the law.

28. We also call on governments and industry to continue to invest in research, development and use of PETs, so that this important field continues to develop and support the free flow of data with trust.

De-identification standards and the place for de-identified data in data protection and privacy law

Prepared by OPC

29. The data protection and privacy authorities of the G7 member countries highlight the importance, both historically and looking ahead to the future, of de-identification as a means to support DFFT, especially given today's data-driven world where the demand for data relating to human activities continues to increase.

30. De-identification tools modify personal information so that it is less likely that an individual can be identified from the information, whether directly or indirectly. The idea, legally and technically, is to transform personal information into a *less* personal form, i.e. to *de*-identify it, while retaining data utility. Examples of de-identification techniques include suppression, generalization and sub-sampling.

31. We underscore that the process of de-identification gives rise to both benefits and risks in relation to privacy. To the extent that de-identification renders personal information less identifiable, it enhances privacy. However, due to the ever-present risk of re-identification, it may pose privacy risks where de-identified information is subject to different rules.

32. We acknowledge the progress made by academia and industry to develop new de-identification techniques, such as differential privacy, and to enhance the capabilities of pre-existing de-identification techniques, such as synthetic data.

33. We as DPAs resolve to continue working towards providing information and advice to stakeholders on appropriate legal and technical standards with respect to the use of these tools in order to achieve an adequate level of data protection. We also commit to continue working towards the development of consistent terminology and/or interoperable definitions of key terms, such as de-identification, anonymization, pseudonymization, and statistical disclosure control.

34. We encourage standardization bodies and communities of practice to continue to support the development of de-identification frameworks, with a view towards establishing robust and common metrics to measuring the risk of re-identification across different contexts and settings.

Reinvigorating the Principles of Data Minimization and Purpose and Use Limitations to Meet the Challenges of Commercial Surveillance

Prepared by FTC

35. Data minimization, the idea that collection should be necessary and proportionate to the purpose for which it has been collected, is a bedrock principle of many of the data protection statutes our agencies enforce. It is a core principle in many data protection and privacy frameworks and laws worldwide. Strong enforcement of that principle coupled with further data use and purpose limitations has the potential to reshape the commercial data ecosystem and address many of its pervasive and emerging harms.

36. Effective enforcement of data minimization principles can right-size the scope of commercial data collection and use to one that meets consumer expectations for a given product on an understandable level.

37. Substantive limitations on data collection and use also play an important role in new legislation being considered by the United States Congress. The American Data Privacy and Protection Act ("ADPPA") currently under consideration in the House of Representatives and similar bills under consideration in the Senate explicitly use the data minimization framework to ensure that data collection and processing is limited to what is necessary and proportionate to provide the service requested by the consumer.

38. Brightline purpose and use restrictions that minimize data collection and use could also mitigate algorithmic harms that we have seen imperil people's civil rights, economic opportunities, and personal autonomy.

39. As the U.S. Federal Trade Commission begins its open inquiry into possibly issuing Trade Regulation Rules on data abuses we hope to learn from and build on the experiences of our peer agencies in effectuating and enforcing these principles.

The role of Privacy and Data Protection Authorities in setting and promoting an ethical and cultural model for AI governance

Prepared by Garante

40. We believe it necessary that the G7 data protection and privacy authorities, as a group of authorities responsible for data protection and privacy of the seven most eminent socio-economic systems in the world, propose a distinctive ethical and cultural model for AI governance.

41. We reject indiscriminate use of AI applied to personal data that results in massive surveillance methodologies with the evident purpose of controlling and manipulating the conduct of individuals – starting from personal data, collected, analysed and cross-referenced in large quantities, variety and speed.

42. The unequivocal and stringent competence of the data protection and privacy authorities on the governance of Artificial Intelligence requires building a virtuous alternative to the use of AI by public authorities that takes into account the values and principles of the rule of law and the democratic government that we all refer to.

43. DFFT requires a position that refuses the use of AI resulting in a massive digital collection of personal data for surveillance purposes and increasingly invasive forms of penetration into the intellectual, spiritual, digital and physical life of citizens.

Next steps towards 2023

44. Building on the results of the Roundtable meeting and the meetings of the Enforcement Cooperation and Technology Working Groups in 2022 we will continue to engage in discussions at expert level with the aim of developing an Action Plan and preparing the Roundtable meeting in which we intend to develop tangible outcomes under the chairpersonship of the PPC, Japan, in 2023.