



# Ministerial Declaration The G7 Digital and Tech Ministers' Meeting 30 April 2023

1. We, the Digital and Tech Ministers of the G7, met on 29 and 30 April 2023 under the chair of Mr. KONO Taro, Minister for Digital Transformation, Mr. MATSUMOTO Takeaki, Minister for Internal Affairs and Communications, Mr. NISHIMURA Yasutoshi, Minister of Economy, Trade and Industry, to address the current and future challenges in the digital society. They also invited for discussion the representatives from the guest countries of Republic of India, Republic of Indonesia, and Ukraine, and the international organisations Economic Research Institute for ASEAN and East Asia, International Telecommunication Union, Organisation for Economic Co-operation and Development, United Nations, and World Bank Group.
2. We, the Digital and Tech Ministers of the G7, once again condemn in the strongest possible terms Russia's war of aggression against Ukraine, which constitutes an unacceptable violation of international law, including the UN Charter. Russia must withdraw all forces and equipment from Ukraine immediately and unconditionally.
3. We reaffirm our commitment from the G7 Digital Ministers' Meeting in Germany last year to support Ukraine and continue to recognise the impact of Russia's war against Ukraine on digital infrastructure. We strongly support the UN Human Rights Council Resolution (A/HRC/49/L.31/Rev.1) led by Ukraine on the 'Role of States in countering the negative impact of disinformation on the enjoyment and realisation of human rights' adopted at the 49th Human Rights Council Session on 1 April 2022.
4. We reaffirm our commitments outlined in the Declaration of the Summit for Democracy, including that the ways in which technologies, including new and emerging ones such as artificial intelligence, biotechnologies, and quantum technologies, are designed, developed, maintained, governed, acquired, funded, sold, and used should be shaped by a commitment to democratic principles including equality, inclusion, sustainability, transparency, accountability, diversity, and respect for human rights including privacy. We underscore the need for technology companies to behave responsibly and reinforce our commitment to the UN Guiding Principles on Business and Human Rights and protect against human rights abuses.
5. Digitalisation and digital infrastructure underpin modern societies and help to deliver inclusive economic growth that maximises the benefits of digital technologies, including emerging technologies and artificial intelligence, such as through the Japanese Presidency's vision for a Society 5.0.

6. In particular, recognising the critical role of data, as an enabler of economic growth, development and social well-being, we advance international policy discussions to harness the full potential of cross-border data flows under the banner of Data Free Flow with Trust (DFFT). In this context, we share the view that trust should be built and realised through various legal and voluntary frameworks, guidelines, standards, technologies and other means that are transparent and protect data. We recognise the need to accelerate and operationalise work on DFFT. We take note of the interests expressed by stakeholders on operationalising DFFT across varied sectors including the areas such as health including pandemic response, climate change, and varied IoT uses including mobility.
7. We recognise that the rapid spread of digitalisation also reveals the necessity to address digital divides both at domestic and international levels. The benefits of emerging technologies can contribute to reducing digital divides including the gender digital divide. We confirm our commitment to strengthen our cooperation with like-minded partners including developing and emerging countries with a view to reducing digital divides including the gender divide, such as by supporting efforts on digital skills and digital connectivity. We recognise that people of all ages and backgrounds need basic digital skills, to enable them to navigate an increasingly digitally connected world and to close digital divides, in cooperation with the G20 Digital Economy Working Group. We also recognise a renewed role for smart city initiatives in promoting connectivity to bridge digital divides in cities and communities of all sizes, based on previous discussions in relevant fora and we look forward to the outcomes of the G7 Sustainable Urban Development Ministers' meeting.
8. Building upon this backgrounds and the outcomes of past G7 Digital and Tech Ministers' meetings, we discussed the facilitation of cross-border data flows and data free flow with trust, secure and resilient digital infrastructure, Internet governance, emerging technologies in innovating society and economy, responsible AI and global AI governance and digital competition.

## **Facilitation of Cross-Border Data Flows and Data Free Flow with Trust**

9. In line with the 2019 G20 Osaka Leader's Declaration, the UK 2021 G7 Roadmap for Cooperation on Data Free Flow with Trust, and the German 2022 G7 Action Plan for Promoting Data Free Flow with Trust, we affirm our commitment to operationalise Data Free Flow with Trust (DFFT) and to build upon commonalities, complementarities, and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust in order to foster future interoperability.
10. We reaffirm our commitment to cooperate on leveraging opportunities of cross-border data flows and addressing challenges raised, in particular, regarding security, privacy protection, data protection, and the protection of intellectual property rights while recognising our varied approaches to data governance. We seek to increase trust across our digital ecosystem and to counter the influence of authoritarian approaches. In this regard, we welcome the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities as a critical tool to improve trust in cross-border data flows by identifying safeguards applicable when clarifying how national security and law enforcement agencies access personal data under existing legal frameworks.

11. We stress the need for tangible progress on advancing DFFT and we recognise that there are potential gaps in international governance to operationalise DFFT in particular due to its cross-sectoral nature, and that there is a need for a new mechanism to bring governments and stakeholders together to cooperate on facilitating cross-border flows of personal and non-personal data under the banner of DFFT. To this end, we commit to operationalising DFFT through a new institutional arrangement for partnership.
12. We resolve to intensify regulatory and technological cooperation and aim to further cooperate on knowledge sharing including through the OECD, the roundtable of G7 data protection and privacy authorities, expert groups relevant to DFFT as well as other multistakeholder forums. We also recognise that the added value of varied perspectives from a range of stakeholders is needed to inform policy efforts. In this regard, we welcome the OECD Report "Moving forward on data free flow with trust: new evidence and analysis of business experiences" as to the issues related to application of privacy and data protection requirements for cross-border data flows, as perceived from a business perspective.
13. To deliver on the goal of operationalising DFFT, we endorse the establishment of the Institutional Arrangement for Partnership (IAP) to bring governments and stakeholders together to operationalise DFFT through principles-based, solutions-oriented, evidence-based, multistakeholder and cross-sectoral cooperation. We endeavour to launch it in the coming months and will convene meetings to further discuss the means under the IAP that could be put in place to achieve our common vision endorsed under Annex 1. We are also committed to working together with international and regional organisations and to support relevant initiatives in a complementary manner. We affirm our commitment to deliver tangible progress in operationalising DFFT and will report to the subsequent meetings of the G7 Leaders and relevant ministers on the outcomes and next steps.

## **Secure and Resilient Digital Infrastructure**

14. Building on the UK 2021 G7 Digital and Technology Ministerial Declaration and the Germany 2022 G7 Digital Ministerial Declaration, we continued and deepened our discussion on secure and resilient digital infrastructure. We recognise the critical role digital infrastructure plays in addressing global challenges such as climate change, pandemics, and fragility.
15. We recognise the importance of continuing work and discussion to enhance security and resilience of digital infrastructure. Rapid digitalisation of the whole society leads to increased demand for higher levels of security and resilience in digital infrastructure in addition to greater speeds, larger capacity, lower energy consumption, lower latency, as well as ubiquitous connectivity. Secure and resilient digital infrastructure is a key foundation for a vibrant economy with high potential for economic growth, job creation and for an open and democratic society. We recognise that network architectures that enhance security and redundancy and promote interoperability can strengthen resilience of digital infrastructure.
16. In line with the 2021 Digital and Technology Ministerial Declaration, we continue to promote secure, resilient, competitive, transparent, sustainable and diverse digital, telecoms, and ICT infrastructure supply chains. We support an innovative and

competitive digital ecosystem which is secure and resilient. We welcome supplier diversification efforts in ICTS supply chains and continue to discuss market trends towards open, interoperable approaches, alongside secure, resilient and established architectures in a technology neutral way. Under the Japanese G7 Presidency and against the background of early deployments of Open RAN, we have exchanged views on open architectures and security-related aspects and opportunities. To further strengthen G7 priorities on secure and resilient digital infrastructure, we are committed to continue working collaboratively within the G7 and with industry and other stakeholders.

17. In order to increase digital infrastructure redundancy, it is important to develop, deploy and maintain various multi-layered networks consisting of terrestrial networks, submarine cable networks, and non-terrestrial networks. We are committed to deepen our cooperation within the G7 and with like-minded partners to support and enhance network resilience by measures such as extending secure routes of submarine cables. Network interoperability is also critical. Ensuring interoperability between various networks to enable roaming between operators in case of an emergency contributes to higher network resilience.
18. It is also important to extend secure and resilient digital infrastructure to like-minded partners, including developing and emerging economies. Developing secure and resilient digital infrastructure globally requires awareness raising of network security, data protection and cloud resilience and thus it is important to strengthen our collective effort to support developing countries in promoting network security including through capacity building.
19. We also recognise the importance of discussion on the role of submarine cable networks and their global development and maintenance, particularly from the security and resilience viewpoint. With the current geopolitical situation in mind, it is urgently important for the G7 to cooperate with other like-minded partners, including those in developing and emerging economies in strengthening global connectivity by ensuring secure and resilient routes of international communication infrastructure.
20. In addition to these efforts to improve security and resilience of current digital infrastructure, we note the importance of sharing a vision for the next generation network in the Beyond 5G/6G era, and endorse the G7 Vision of the future network in the Beyond 5G/6G era. We are committed to enhancing cooperation on research, development, and international standards setting, toward building digital infrastructure for the 2030s and beyond. [Annex 2]
21. We endorse the G7 Action Plan for Building a Secure and Resilient Digital Infrastructure that outlines the above efforts to build a secure and resilient digital infrastructure. In supporting secure and resilient digital infrastructure in developing countries, we seek to cooperate with international organisations and development agencies such as the World Bank and the ITU. [Annex 3]

## **Internet Governance**

22. We reconfirm our commitment to the promotion of an open, free, global, interoperable, reliable, and secure Internet that supports innovation and strengthens respect for democratic values and human rights. We also confirm our commitment to the protection

and promotion of one global, unfragmented Internet and thus oppose any intention and action toward Internet fragmentation.

23. We strongly support and promote the inclusive multistakeholder approach to Internet governance. We reinforce our support for the UN Internet Governance Forum (IGF) as the leading multistakeholder forum for Internet policy discussions. We are committed to making collective efforts toward the success of IGF 2023 in Kyoto, Japan, including stronger collaboration with stakeholders from national, regional and global stakeholder communities.
24. We reconfirm our commitment to the Declaration for the Future of the Internet (DFI) and its principles, and to cooperating in implementing them. We also continue to strive to expand this commitment within the global family of countries that also support democratic values, aiming for a global protection of the DFI's crucial principles that underpin today's open and free Internet. We welcome DFI's geographic and economic diversity, including developing countries and emerging economies and invite the global community to join the effort. In this regard, we continue to strengthen our collaboration with stakeholders around the world in implementing DFI and its principles.
25. We condemn government-imposed Internet shutdowns and network restrictions. We resolve to cooperate in making visible and tackling the tactics of digital authoritarianism, and seek to strengthen cooperation in addressing practices such as Internet shutdowns, network restrictions and digital mass-surveillance that violate international human rights law, including by collaborating with other initiatives such as the Freedom Online Coalition and its Task Force on Internet Shutdowns. We are committed to protect the technical infrastructure essential to the general availability or integrity of the Internet.
26. We endorse the G7 Action Plan for an Open, Free, Global, Interoperable, Reliable and Secure Internet. [Annex 4]
27. We remain committed to protecting our democratic institutions and values from foreign threats, including foreign information manipulation and interference, disinformation and other forms of foreign malign activity that seek to undermine democracy and the ideals that open societies are founded on, consistent with existing initiatives, including the G7 Rapid Response Mechanism (RRM), the G7 Interior and Security Ministers' Meeting, and the OECD MIS/DIS Information Resource Hub.
28. Information integrity is a challenge in strengthening trust in the digital economy with broader societal implications. We recognise the importance of actions taken by a wide range of stakeholders, including social media platforms, civil society, the Internet technical community, and academia to address online information manipulation and interference and disinformation while respecting human rights, in particular to the right to freedom of expression. We plan to collaborate in gathering and compiling existing practices by various stakeholders to address online disinformation as Existing Practices against Disinformation (EPaD), and intend to publicise and present this report at the UN IGF 2023 in Kyoto. Some of these practices include stopping monetisation of disinformation content, strengthening the accountability of digital platforms, or providing users with the means to understand and report disinformation. We also encourage businesses to allocate adequate resources which reflect the diversity of languages and cultures where they operate when it comes to countering intentional online information

manipulation and interference, including disinformation.

29. We are committed to work together with all stakeholders to contribute to the UN Global Digital Compact (GDC), with a view to promoting a human rights based, and gender responsive approach, and with reference to existing outcome documents such as the Agreed Conclusions of the 67th session of the Commission on the Status of Women on gender equality in innovation and technology, and international human rights law commitments, including in relation to gender equality. We will encourage the GDC to reinforce build on, and contribute to the success of the IGF and WSIS process. Based on our commitment to the multistakeholder approach, we also resolve to work together to prepare for the coming discussions during the WSIS+20 review process in 2025, including empowering multistakeholder participation and engagement.

### **Emerging and Disruptive Technologies in Innovating Society and Economy**

30. We recognise that digital innovation accelerated by emerging technologies and innovative governance models has the power to unlock inclusive economic growth and a sustainable society that serves the well-being of people. We also recognise the importance of developing cyber and digital skills across the economy. To ensure that we are able to capitalise on the benefits of emerging technologies, including integration of cyber-physical systems and its major components including Internet of Things (IoT) technology, we work toward social implementation of emerging technologies, embedding security within technology and ensuring domestic and international interoperability of technologies composing digital infrastructures.
31. We share the importance of developing policy discussions on digital identity systems and other means to build trust and security in data sharing. We will share and accelerate best practices on digital identity and credentials and support discussions on the ongoing development of the OECD draft recommendation on the governance of digital identity. We take note of the discussions at the G7 Stakeholder Conference on Digital Technologies for Trust on 29 March 2023 on compatible policy approaches and technologies for data exchange in a trusted way, including enhanced traceability and controllability of data as well as verification of data sharing partners.
32. We recognise that hardware and software across sectors and borders are intricately interconnected as a system, and hence we need to cooperate throughout the global value chain of digitally-enabled products and services to enable trust and security in the digital economy. In this regard, we recognise interoperability based on trust of software and IoT products contributes to managing existing and potential vulnerabilities. We recognise the importance of designing, developing, and deploying well-secured apps and software and responding to vulnerabilities appropriately, including by enhancing transparency of software components.
33. We also affirm the importance of foundational digital technologies, such as semiconductors, and exploring the value technical standards could provide to minimise the impacts of a supply chain disruption. We recognise the need to continue working with stakeholders across the G7 and like-minded countries in relevant forums on emerging technology topics, such as interoperability of IoT products in cooperation with relevant Ministerial tracks.

34. We share the view that rapid innovation of emerging and disruptive technologies that allows us to boost the economy and address varied social challenges such as climate change, pandemics, and the effects of aging populations, in turn requires consideration regarding governance of digital technologies and examination of societal impacts including to address misuse. In this regard, we acknowledge the need for agile, more distributed and multi-stakeholder governance and legal frameworks, designed for operationalising the principles of the rule of law, due process, democracy, and respect for human rights while harnessing the opportunities of innovation. We acknowledge the need for a possible common approach on this agenda based on the input by the Taskforce on Governance for a Digitalized Society with a view to enabling human-centred, sustainable, and resilient societies by benefit of technologies.
35. We also acknowledge the call of the multistakeholder community at the G7 Digital Transformation Summit held on 28 April 2023 where they discussed with G7 Ministers the key issues of digital transformation including artificial intelligence, digital infrastructures, and agile governance based on the delivery of Governance Principles for a Society based on Cyber Physical Systems by the Taskforce. We recognise the need to consider the suggestions by stakeholders in the related works of the G7 Digital and Tech. We also welcome the establishment of the OECD Global Forum on Technology as an important new forum to bring together multiple stakeholders around emerging technology impacts and opportunities.
36. We reiterate our long-term commitment to better harness digital technologies to achieve a sustainable society and continue working on green transition, energy and resource efficiency, circular economy and climate change in digitalising society while working to mitigate the environmental impacts of the digital sector itself.  
These efforts include:
- > Improving circularity of hardware and energy efficiency on data centres and next generation computing including software technologies by improving computational velocity and efficiency.
  - > Collaboratively exploring opportunities to leverage a life cycle approach in developing, implementation and use of digital technologies including the recyclability and “right to repair” these technologies.
  - > Exchange best practices and advance a sustainable by design approach of digital equipment and products in order to reduce the consumption of resources and increase the use of recycled elements in these products of sustainable by design.
37. We also call for development of sustainable supply chains and seek to explore the potential impact thereof. In this regard, we work on:
- > Sharing information on the use, reuse, and disposal of hazardous substances and compounds used in production of IoT, semiconductors and other digital equipment and possible means of alternation.
  - > Improvements of the circularity of these supply chains and any potential environmental impacts.
38. We continue discussions on the ways to develop our collective approaches on immersive technologies such as the metaverse. We recognise the potential of immersive technologies to provide a myriad of innovative opportunities for different areas and use cases and the need for policy discussions on interoperability, portability, and ecological

sustainability and standards to support these aims as well as to foster a trustworthy, safe and secure use of the technologies based democratic values while maintaining a free open and fair global economic architecture. We recognise the role that international organisations could play in this regard and seek to continue contributing to on-going discussion in relevant multilateral fora including the OECD.

## **Responsible AI and Global AI Governance**

39. In 2016, we initiated an international discussion on AI principles. This discussion helped pave the way for the 2019 OECD AI Recommendation (OECD AI Principles) and the associated work launching the OECD.AI Policy Observatory and Network of Experts. In 2020, we supported the launch of the Global Partnership on Artificial Intelligence (GPAI).
40. The OECD AI Principles provide guidance for trustworthy AI and for ensuring an open and enabling environment for AI development and deployment that is grounded in human rights and democratic values. Since adoption of these principles, the OECD continues to engage and work with the global AI community to support their implementation.
41. Rapid AI developments call for attention to, and cooperation on, emerging and medium-term policy issues including development of technical standards, developed by international standards development organisations (SDOs), as well as other tools to ensure the development and deployment of trustworthy AI in line with the OECD AI Principles. In this context, we welcome the contributions of existing initiatives on these topics.
42. We reaffirm our commitment to promote human-centric and trustworthy AI based on the OECD AI Principles and to foster collaboration to maximise the benefits for all brought by AI technologies. We oppose the misuse and abuse of AI to undermine democratic values, suppress freedom of expression, and threaten the enjoyment of human rights.
43. We stress the importance of international discussions on AI governance and interoperability between AI governance frameworks, while we recognise that like-minded approaches and policy instruments to achieve the common vision and goal of trustworthy AI may vary across G7 members. Tools for trustworthy AI, such as regulatory and non-regulatory frameworks, technical standards and assurance techniques, can promote trustworthiness and can allow for the comparable assessment and evaluation of AI systems. We support the development of tools for trustworthy AI through multistakeholder international organisations, and encourage the development and adoption of international technical standards in SDOs through private sector-led multistakeholder processes. We commend work to date in the OECD on mapping the commonalities and differences between trustworthy AI frameworks, and we intend to work together to support such work that fosters interoperability.
44. We are committed to supporting all stakeholders from across sectors, with their participation in SDOs, and to facilitating inclusive engagement with a special emphasis on participation of SMEs, start-ups, academia and wider society. We resolve to promote international technical standards to support interoperable tools for trustworthy AI.
45. We reaffirm that AI policies and regulations should be human centric and based on



democratic values, including protection of human rights and fundamental freedoms and the protection of privacy and personal data. We also reassert that AI policies and regulations should be risk-based and forward-looking to preserve an open and enabling environment for AI development and deployment that maximises the benefits of the technology for people and the planet while mitigating its risks.

46. We recognise that AI development is progressing rapidly, and has the potential for significant impacts on society. Being mindful of such potential impact of AI on our societies, we also recognise that AI policies and regulations should be adapted to the context of application in a way that is sensitive to technical and institutional characteristics as well as societal and cultural implications, including geographic, sectoral and ethical aspects.
47. Given that generative AI technologies are increasingly prominent across countries and sectors, we recognise the need to take stock in the near term of the opportunities and challenges of these technologies and to continue promoting safety and trust as these technologies develop. We plan to convene future G7 discussions on generative AI which could include topics such as governance, how to safeguard intellectual property rights including copyright, promote transparency, address disinformation, including foreign information manipulation, and how to responsibly utilise these technologies. These discussions should harness expertise and leverage international organisations such as the OECD to consider analysis on the impact of policy developments and GPAI to conduct relevant practical projects.
48. We endorse the Action Plan for promoting global interoperability between tools for trustworthy AI and for cooperating to anticipate and prepare for upcoming AI opportunities and challenges. [Annex 5]

## **Digital Competition**

49. Digital markets are global, dynamic, can involve novel business models and large amounts of data, and have a vital and important impact on the competition and innovation in our economies. It is increasingly important to both use existing competition enforcement tools and to develop and implement new or updated competition policy initiatives or regulatory and competition frameworks, which may be required to complement or adjust the existing competition policy instruments, swiftly and effectively to address the issues caused by entrenched market power, promote competition and stimulate innovation. This may be particularly important in connection with fostering fairness and contestability. In recognition of this importance, we acknowledge that digital competition is a global issue requiring cooperation by enforcers and policymakers.
50. We resolve to further strengthen cooperation based on the knowledge accumulated and shared by the G7 chaired by France, the United Kingdom, and Germany. We intend to share issues and challenges that G7 members are facing in promoting digital competition, such as those common to G7 members in using, implementing, and planning existing, new and upcoming laws and regulatory tools.
51. We plan to also update the “G7 inventory of new rules for digital markets”, the mapping of legal approaches to digital competition in each of the G7 jurisdictions to facilitate

mutual understanding in sharing the above with a view to fostering greater coordination to support competitive digital markets.

52. We intend to share the experiences that G7 members have in their respective jurisdictions with respect to competition in digital markets, including enforcement, and discuss how G7 enforcers and policymakers can cooperate for a better understanding of the approaches to digital competition oversight. We plan to also update the “Compendium of approaches to improving competition in digital markets” in the G7 and other jurisdictions.
53. We plan to convene a summit related to digital competition for competition authorities and policymakers in the fall of 2023 to facilitate international efforts to promote competitive markets and effective competition law enforcement.
54. In addition to convening an enforcers’ and policymakers’ summit in the fall of 2023, we also plan to create a point of contact group to facilitate the close exchange of information and experience among the G7 competition authorities and policymakers throughout the year.

## **Way Forward**

55. We express our appreciation to our knowledge partners ERIA, ITU, OECD, UN, and the World Bank for contributing their expertise and experience, and welcome continuous cooperation to realise a prosperous, digitally connected world based on our shared democratic values.
56. We encourage the G7 Leaders to take note of our discussions during the G7 Summit in Hiroshima from 19 to 21 May 2023.
57. We express our continuous support and solidarity with Ukraine in light of Russia’s illegal invasion and infringement of international law.
58. We discussed the potential of digital technologies to address sustainability challenges, including mitigation of the environment impacts of the digital sector itself. Looking ahead, we encourage continued G7 discussions on these issues.
59. We look forward to Italy’s G7 presidency in 2024 and encourage the G7 to continue building on the outcomes of Japan’s 2023 G7 presidency and its positive and ambitious legacy.