G20 Digital Economy Ministers Meeting

Ministerial Declaration

Wednesday, July 22, 2020

1. Building on the achievements and commitments of past Presidencies, we, the G20 Ministers responsible for the digital economy, met on 22 July 2020 to discuss harnessing digital technologies to realize opportunities of the 21st century for all. In 2020, the G20 Digital Economy Task Force (DETF) brought together all G20 members as well as guest countries. Saudi Arabia also invited the Organisation for Economic Co-operation and Development (OECD) and the International Telecommunication Union (ITU) as knowledge partners.

2. As our societies and the global economy digitalize, there are ever greater opportunities to advance standards of living through human-centric, data-driven, and evidence-based policy, increased economic competitiveness, higher-quality jobs, enhanced provision of public services in cities of all sizes and communities in remote and rural areas, and more inclusive societal participation of people from all backgrounds. Digitalization also poses challenges including how to bridge digital divides, and develop effective policies and strategies, that are innovative as well as agile, flexible, and adapted to the digital era, while addressing anti-competitive practices, safeguarding privacy, advancing security, building trust, and reducing inequalities. Digitalization is also increasing the importance of boosting job opportunities, increasing market access for Micro, Small and Medium Enterprises (MSMEs). We support fostering an open, fair, and non-discriminatory environment, protecting and empowering consumers, ensuring the safety and stability of supply chains in relevant areas, and advancing inclusiveness and human-centricity more broadly, noting the importance of the environmental impact of digitalization and introducing a gender lens. We continue to support international cooperation and multi-stakeholder engagement to design and implement evidence-based digital policies to address these challenges. We recognize that various countries have already taken steps with the intention of making policy approaches more flexible, holistic, and agile, for example through the use of regulatory sandboxes.

3. We stress the importance of the digital economy and policy discussions to sustain progress on the implementation and achievements of the 2030 Agenda for Sustainable Development.

4. We recognize that universal, secure, and affordable connectivity is a fundamental enabler of the development of the digital economy and a catalyst for inclusive growth, innovation, and sustainable development. We recognize the importance of initiatives related to advancing digital connectivity infrastructure, digital skills and awareness, the affordability of Internet services and devices, closing the digital gender gap, and the relevance of digital content. We recognize the need to close the gaps in these areas and the importance of working with stakeholders to connect humanity by accelerating global Internet penetration, especially in remote and rural areas.

5. We emphasize the role of connectivity, digital technologies, and policies in accelerating our collaboration and response to the COVID-19 pandemic and enhancing our ability to prevent and mitigate future crises as stated in our Extraordinary Statement adopted on April 30, 2020. We note the Policy Options to Support Digitalization of Business Models during COVID-19, developed by the Saudi

Presidency, which shares policies and practices to strengthen business continuity and resilience consistent with national circumstances.

I. Trustworthy Artificial Intelligence

6. Artificial Intelligence (AI) systems have the potential to generate economic, social, and health benefits and innovation, drive inclusive economic growth, and reduce inequalities as well as accelerate progress toward the achievement of the Sustainable Development Goals (SDGs). They could also have potential impacts on the future of work, the functioning of critical systems, digital inclusiveness, security, trust, ethical issues, and human rights.

7. We reaffirm our commitment to promoting a human-centered approach to AI and support the G20 AI Principles, which are drawn from the OECD AI Principles – including section 1, Principles for Responsible Stewardship of Trustworthy AI, and section 2, the Recommendations on National Policies and International Co-Operation for Trustworthy AI. We each commit to advance the G20 AI Principles, in accordance with national priorities.

8. As a first step, we note the Examples of National Policies to Advance the G20 AI Principles (Annex 1), which presents a list of examples of national strategies and policy approaches to advance the G20 AI Principles, including investment in research, human capacity, innovation, and trustworthiness.

9. We believe that there is a need for inclusive multi-stakeholder discussions and sharing of experiences on AI and related policy practices. We welcome the Dialogue hosted by the Saudi Presidency on trustworthy AI in pandemic response and note the Summary of Discussions from the G20 AI Dialogue in 2020. We promote continued multi-stakeholder discussions on AI, consistent with the G20 AI Principles.

II. Data Free Flow with Trust and Cross-Border Data Flows

10. In 2019, in Osaka, G20 Leaders acknowledged the importance of data free flow with trust and cross-border data flow and recognized the critical role played by effective use of data for digitalization, as enablers of economic growth, development, and social well-being, and expressed their willingness to cooperate to encourage the interoperability of different frameworks and reaffirmed the role of data for development.

11. The cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. At the same time, we recognize that the free flow of data raises certain challenges, such as the protection of privacy and personal data. G20 members recognize the need to address these challenges, in accordance with relevant applicable legal frameworks, which can further facilitate data free flow and strengthen consumer and business trust, without prejudice to legitimate public policy objectives,

including by:

- sharing experiences and good practices for data policy, in particular interoperability and transfer mechanisms, and identifying commonalities between existing approaches and instruments used to enable data to flow across borders with trust;
- reaffirming the importance of the interface between trade and digital economy, noting the ongoing negotiations under the Joint Statement Initiative on electronic commerce and reaffirming the importance of the Work Programme on electronic commerce at the WTO;
- exploring and better understanding technologies such as privacy enhancing technologies (PETs).

III. Smart Cities

12. Building on the achievements of past Presidencies, we encourage further work with stakeholders for the development and deployment of digital technologies and solutions for human-centric, environmentally sound, sustainable, rights-respecting, and inclusive smart cities and communities that boost competitiveness and enhance well-being and community resilience. These digital solutions should be centered around connectivity and providing services in more efficient and personalized ways, while safeguarding human rights. These digital solutions should also be deployed responsibly with effective security and resilience in the digital economy to safeguard privacy, personal data, and service provision, and foster greater transparency and public trust. In this respect, we take note of the G20 Global Smart Cities Alliance initiative launched in 2019.

13. We recognize that smart mobility is one of the elements of a holistic approach to smart cities and communities, serving as a vital engine of innovation and investment, and that smart mobility data and technology solutions can address some of the challenges of smart cities and communities, potentially reducing inequality of access to cities' services in an environmentally friendly way.

14. We welcome the G20 Smart Mobility Practices (Annex 2) to contribute to this work. Its purpose is to provide guidance and best practices regarding how to accelerate the diffusion of smart mobility systems in ways that are human-centric, inclusive, and sustainable, based on experiences and shared knowledge of G20 members and beyond.

15. We recognize the work of G20 members to facilitate smart mobility technology and digital infrastructure deployment, build the digital capacity of governments, promote interoperability, monitor the impacts of smart mobility including those on human rights, foster multi-stakeholder collaboration and partnership, and cultivate and promote digital inclusion.

16. Going forward, we recognize the importance of aligning work on smart cities with the G20 Infrastructure Working Group and advancing smart cities and

communities' approaches, in cooperation with local partners and other relevant social partners. We encourage the exploration of other elements of smart cities and communities beyond smart mobility.

IV. Measurement of the Digital Economy

17. Building on the work carried out under previous G20 Presidencies and following up on the draft 2018 G20 Toolkit for Measuring the Digital Economy, developed under the Argentine Presidency, we support advancing digital economy measurement. Reinforced cooperation will help advance consistency across different approaches and enhance evidence-based policymaking to contribute to the realization of the opportunities of the 21st century for all.

18. We welcome the G20 Roadmap toward a Common Framework for Measuring the Digital Economy (The Roadmap, Annex 3) developed under the Saudi Presidency. The Roadmap contributes to closing measurement and implementation gaps, especially in developing economies, and to strengthening comparability of indicators, as well as statistical capacities in G20 countries and beyond. We promote inclusive and multi-stakeholder dialogue on measurement and recognize the contributions made during the G20 Workshop on Measurement of the Digital Economy.

19. We acknowledge the importance of exchanging information on how best to define elements of the digital economy to guide measurement efforts. Building on the outcomes reached in Hangzhou in 2016, and the established frameworks of statistical accounting in sectors and industries, G20 countries this year recognize the proposal by the Saudi Presidency of a tiered definitional framework that supports the following overarching policy definition of elements of the digital economy, for measurement purposes: the digital economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services, and data; it refers to all producers and consumers, including government, that are utilising these digital inputs in their economic activities.

20. In order to improve our ability to monitor the social and economic impact of the digital economy, and evaluate policies to shape its evolution while ensuring that no one is left behind, including women and girls, we recognize the importance of representative indicators related to jobs, skills, including digital literacy, and growth, and their effective use across communities, taking into consideration the distribution of outcomes across gender, education, and other socio-economic factors wherever practicable. To improve data availability and current statistics and to strengthen the evidence base in measuring the digital economy, we support working with relevant stakeholders such as the private sector, business entities, educational institutions, civil society, and International Organizations, to consider identifying, developing, and using new and existing sources of data, including gender- or sex-disaggregated data, in accordance with national practices, where it does not yet exist, while protecting privacy and personal data.

21. New business models enabled by digital transformation present various measurement challenges related to data, digital services, and digital platforms. We encourage the discussion and exploration of indicators to account for various measurement challenges, providing measurement guidance where possible, and recognizing efforts to integrate the digital economy into the national accounts and other statistical systems, where appropriate.

22. We recognize the progress made to date and encourage further work on the priority areas identified by the Roadmap.

V. Security in the Digital Economy

23. In 2017, we acknowledged that trust and security are vital to harnessing the potential of the digital economy. In the context of rapidly expanding digitalization and the spread of advanced technologies, enhancing security in the digital economy is increasingly important. Building on our past discussions, in 2020 we commit to working with all stakeholders to advance security in the digital economy in the service of our shared economic interests. By working together, we can help mitigate security risks in the digital economy and reduce systemic risk, contributing to the advancement of strong, sustainable, and inclusive global economic growth.

24. This year the Saudi Presidency hosted a G20 Cybersecurity Dialogue dedicated to inclusive multi-stakeholder, cross-sectoral discussion of the security risks and challenges, as well as opportunities, that characterize the digital economy. Discussions focused on ways in which inclusive capacity-building can support efforts to strengthen security in the digital economy, in particular in micro, small, and medium sized enterprises.

25. We recognize efforts by the Kingdom of Saudi Arabia to create multi-stakeholder dialogue and advance progress in addressing the complex challenges of the digital domain, including through the 2020 Global Cybersecurity Forum.

26. Recognizing that security in the digital economy is central to risk management strategies of all businesses, and highlighting the important place of MSMEs as elements of global value chains, in particular in the global economic response to COVID-19, we welcome the G20 Examples of Practices Related to Security in the Digital Economy (Annex 4), which highlights governmental programs and initiatives. This Annex includes examples provided by governments of policies related to resilience in the digital economy. We encourage all organizations to integrate the relevant aspects of resilience in the digital economy into their overall security risk management strategies, while preserving and respecting human rights. We promote continued multi-stakeholder discussions to advance security in the digital economy.

VI. Way Forward

27. We recognize the role of engagement groups, the interlinkages between our workstreams, and the importance of sharing ideas, experiences, and best practices, as well as practical solutions with all interested parties. We thank the International Organizations, that were invited by the Saudi Presidency, including the Organisation for Economic Co-operation and Development (OECD), International Telecommunication Union (ITU), International Labor Organization (ILO), International Monetary Fund (IMF), United Nations Statistics Division (UNSD), and the United Nations Conference on Trade and Development (UNCTAD), for their contributions.

28. We recognize that the digital economy has and will continue to have wide-ranging implications as a driver of inclusive economic growth and development, contributing to the achievement of the Sustainable Development Goals, and as a means to prevent and address crisis situations and aid businesses and industry in recovering from the impact of COVID-19. We acknowledge the crosscutting impact of the digital economy in overcoming development challenges, including growth, labor, employment, social, health, and cultural challenges. We therefore welcome continued discussion of the transformation of the Digital Economy Task Force to a Digital Economy Working Group.

Annex 1: Examples of National Policies to Advance the G20 AI Principles

The purpose of these Examples of National Policies to Advance the G20 AI Principles (Examples) is to provide countries with examples of national policies as they advance the G20 AI Principles. This Annex provides a stylized mapping against the G20 AI Principles and is based on a stocktaking exercise undertaken under the Saudi G20 Presidency with the support of the OECD. Countries were asked to highlight selected examples of policies that aim at, or have the effect of, advancing the G20 AI Principles. All general descriptions below thus draw from these current active efforts to advance trustworthy AI, representing a source of knowledge exchange.[1] The inclusion of examples in the list below does not imply endorsement by G20 countries of the policies described therein.

This Annex accounts for different contexts and experiences, is non-exhaustive, and is not meant to be prescriptive. The diversity of the Examples suggests that much activity and experimentation is taking place to build and support AI ecosystems. Most strategies and policies are recent or still in the process of being developed. Many seem to address, explicitly or implicitly, multiple G20 AI Principles at once, which is consistent with the intent of the Principles to be complementary and mutually reinforcing. Few policies have existed for long enough to conduct evaluations. This suggests that there is scope for sharing experiences to facilitate learning, including by promoting multi-stakeholder discussions on AI, consistent with the G20 AI Principles.

Principles for the Responsible Stewardship of Trustworthy AI

G20 countries are undertaking wide-ranging action to encourage the responsible stewardship of trustworthy AI. They are advancing, among others, the following actions related to the five values-based G20 AI Principles:

1. **Inclusive growth, sustainable development and well-being:**
   - **Elaborating AI strategies** that take a coherent whole-of-society approach to AI development and use. Such strategies can set a shared vision and overarching objectives and often address multiple G20 AI Principles. They can also propose directions for sectors considered critical for human development.
   - **Formulating national AI plans** that guide public policies, initiatives and practices over the medium-term, and which may set specific objectives, encompass multiple policy instruments, and draw on multi-stakeholder governance structures.
   - **Drafting AI-related guidance, governance models, frameworks, and principles** that set out high-level requirements for trustworthy AI systems. These may benefit from the collection and sharing of practical use cases, examples, and best practices.

2. **Human-centered values and fairness:**
   - **Setting AI ethics principles** that place emphasis on safeguarding human rights and promoting fairness across groups in society. Such principles can guide businesses and governments as they design, develop and deploy AI, and may incorporate both expert input and public consultation to build broad societal support.
   - **Preparing directives and guidelines for AI implementation by governments**. This may include specification of key characteristics of AI technical standards that agencies should consider as well as guidance on regulatory and non-regulatory approaches to technology and sectors enabled by AI.
   - **Drafting implementation and self-assessment guides.** To operationalize principles, countries are piloting practical guidance (e.g. assessment lists or tools) with stakeholders to better pinpoint where ethical issues will arise and how specific AI

[1] The background report 'Examples of AI National Policies' was produced by the OECD for the G20 Saudi Presidency. The opinions expressed and arguments employed in this report do not necessarily represent the official views of the member countries of the G20.

applications may be tailored to promote human-centricity, fairness, and proper governance. Such guides may also identify industry best practices that organizations can refer to.

3. **Transparency and explainability:**
   - **Issuing directives and guidelines for AI implementation**, including automated decision-making processes, and seeking to ensure compatibility with key legal principles of transparency, accountability, legality and procedural fairness.
   - **Providing implementation and self-assessment guides** that include mapping of key considerations and practices related to AI deployment, and providing examples of good practices.

4. **Robustness, security and safety:**
   - **Addressing robustness, security and safety as part of directives and guidelines for AI implementation** by governments and in guides for organizations. This can include elements related to risk management, testing and constant learning, and draw on industry examples and practices.
   - **Encouraging R&D into practical tools** for promoting robustness, security and safety in AI systems.

5. **Accountability:**
   - **Addressing accountability as part of directives and guidelines for AI implementation** which can include considerations and practices related to internal governance structures, as well as providing industry examples and practices.
   - **Encouraging R&D into practical tools** for promoting accountability in AI systems.

National Policies and International Co-operation for Trustworthy AI

G20 countries are actively experimenting with national policies and engaging in international co-operation to promote trustworthy AI by, among others, the following actions related to the five recommendations for policy included in the G20 AI Principles:

6. **Investing in AI research and development:**
   - **Developing AI R&D strategies and plans**. These take a comprehensive view across AI technology, skills and infrastructure and set a coherent pathway, with objectives related to e.g. competitiveness, scientific leadership and innovation.
   - **Formulating AI technology roadmaps to guide investment**. These can identify domains of AI development and application that are considered of particularly high potential in the country context.
   - **Supporting AI research and excellence centers**. These can contribute to practical solutions and applications that serve to promote trustworthy AI and can promote private-public collaboration. This may also contribute to fostering the AI ecosystem and developing human capacities.
   - **Funding AI R&D projects and programs** by launching calls or awarding grants for R&D projects that may seek to underpin multidisciplinary research by encouraging collaboration across relevant fields, which could include MSMEs.
   - **Developing AI standards roadmaps** to improve interoperability and use of standards.
   - **Issuing technical standards plans for AI** that provide guidance to government agencies regarding their adoption, development or monitoring of technical standards in regulatory or procurement actions. These may define important characteristics of such standards.

7. **Fostering a digital ecosystem for AI:**
   - **Creating robust data ecosystems and data authorities** that could provide overarching guidance on data usage and sharing, personal data protection and privacy, ethics and data-driven innovation, as well as advice and direction on possible regulatory and non-regulatory approaches to data.
   - **Fostering open and synthetic data initiatives**. For example, this could establish open data portals for access to data produced by public resources, alongside data infrastructure and analytics.

8. **Shaping an enabling policy environment for AI:**
   - **Establishing advisory councils for AI** to advise on priorities for AI development and deployment (under the overarching objectives) and play a role in public consultation and international collaboration.
   - **Creating national AI centers to contribute to AI innovation and capacity building** and take a role in promoting implementation of a national AI strategy, undertaking AI research, developing AI applications and supporting AI workforce education and training.
   - **Providing guidance for regulation of AI applications** to inform development of regulatory and non-regulatory approaches towards technologies or industry sectors that are empowered or enabled by AI, with a view to providing regulatory certainty and improving the environment for innovation.

9. **Building human capacity and preparing for labor market transformation:**
   - **Establishing education programs for children** to build digital literacy, and develop AI-specific skills and capabilities such as statistical thinking, mathematics and comprehension of AI outcomes. Programs may include efforts to provide relevant infrastructure and resources to students.
   - **Supporting skills development for people of all ages**, including through provision of financial support and high-speed infrastructure development to ensure inclusive and creative learning in school, and certification of education programs related to mathematical science, data science and AI, and provide access to training programs from the public or private sector.
   - **Promoting research on the impact of AI on work and employees**. Such research may involve collaboration with business and labor unions and can look at the effects of AI adoption in the workplace, the automation of jobs, the impact on job quality and experience, and implications for skills and task evolution.

10. **International cooperation for trustworthy AI:**
    - **Engaging in the work of international organizations** to leverage research and dialogue at the international level. This can foster knowledge-sharing, understanding of national contexts, and development of shared approaches on relevant issues.
    - **Engaging in dialogue on AI standards development work**. This can foster interoperability and knowledge sharing on critical technical standards for AI.
    - **Promoting multi-stakeholder initiatives** to foster international collaboration and pursue specific projects that contribute to the responsible development of AI, grounded in human rights, inclusion, diversity, innovation and economic growth.

Annex 2: G20 Smart Mobility Practices

The purpose of this document is to provide evidence-based guidance and practices regarding how to leverage digital technologies and data to accelerate the diffusion of smart mobility systems, based on experiences and shared knowledge of G20 members and beyond. They include policies that governments at the national, regional, and local levels could consider regarding the integration of smart mobility within broader smart cities and communities' strategies, deployment of technology and digital infrastructure, measurement, data governance, interoperability, capacity building, multi-stakeholder collaboration, and frameworks.[2]

To leverage digital technologies and data to accelerate the diffusion of smart mobility systems that are human-centric, rights-respecting, inclusive, resilient, and sustainable, G20 countries could consider policies that:

1. Integrate smart mobility within a broader strategy for human-centric, rights-respecting, inclusive, accessible, and sustainable smart cities and communities

Adopt an integrated and holistic approach to smart mobility planning that is human-centered and contributes to social inclusion. Plan smart mobility strategies with an integrated and holistic perspective in relation to how digital technology and data are likely to change mobility and people's mobility behaviour in the coming years, articulating smart mobility policies with other smart cities and communities' policies and the Sustainable Development Goals to ensure inclusiveness, well-being, and equal accessibility, including reducing the physical and social barriers to access goods and services for women, the elderly, people with disabilities, the youth, as well as people from different levels of income, digital skills, or social backgrounds.

Address local contexts, conditions and capacities, aligning smart mobility investment with communities' development goals and people's needs. Plan and design context-sensitive smart mobility models that align with communities' development goals, government capacity, available funding, and people's needs, and engage with people from the early stages of the decision-making process to build trust.

Assess the accessibility of smart mobility solutions from the outset of the policy process. Consider people's ability to access and navigate smart mobility digital channels and services effectively, including expansion of broadband infrastructure, especially in poorly served areas, including remote and rural areas, and among vulnerable groups, including persons with disabilities, and strengthening people's basic digital skills, such as using a smartphone and keeping their personal data secure.

2. Facilitate and guide smart mobility technology and digital infrastructure deployment

Maintain a neutral stance with respect to smart mobility technology and infrastructure development and deployment. Adopt a prudent, neutral, and future-proofing stance and avoid making all-in bets on technology, exploring open source solutions where appropriate, including mechanisms to re-examine decisions periodically and adapt or re-direct as required.

Deploy a risk-based assessment framework for smart mobility technology and infrastructure. Support conformity assurance regimes to guarantee smart mobility systems enhance safety and efficiency and contribute to improved environmental impacts and social outcomes.

[2] The background report 'Leveraging Digital Technology and Data for Human-centric Smart Cities' was produced by the OECD for the G20 Saudi Presidency. The opinions expressed and arguments employed in this report do not necessarily represent the official views of the member countries of the G20.

Adopt a security by design approach for smart mobility to mitigate security and safety risks. Follow security by design principles and address the functional isolation of all core safety-critical components of smart mobility systems to mitigate security and connectivity risks and make safety performance independent from access to shared external communication channels alone.

Promote evidence-based principles to guide the impact assessment of algorithmic decision-making for smart mobility solutions. Promote principles to undertake risk-based, evidence-based algorithmic system impact assessments, aligned with the G20 AI Principles, to guide potential smart mobility interventions in areas where clearly demonstrated harms may exist and audit these assessments based on observable and monitored impacts.

Anchor smart mobility at the heart of pro-resilience frameworks. Articulate smart mobility systems within a larger set of pro-resilience frameworks that may enable rapid reaction and timely recovery from system shocks, including how to swiftly deliver emergency services, prioritise access, minimise contagion risks, and ensure rapid but orderly recovery efforts, among others.

Promote innovation and invest in supporting digital infrastructure. Allocate resources for investing in innovation and supporting digital infrastructure, including connectivity and adapting public space, implementing public procurement processes for smart mobility solutions when appropriate, and leveraging public-private partnerships, where appropriate.

3. Measure and monitor impacts of smart mobility within a data governance framework

Consider mobility data within a broader context of general data governance. Align the collection, processing, ownership, use and destruction of mobility data with broader data governance principles and frameworks, where these have been defined, prioritizing development of industry-led, voluntary, consensus-based, international technical standards to support mobility data governance.

Deploy a multi-indicator assessment framework to monitor the contribution of smart mobility to public policy outcomes. Develop robust monitoring frameworks spanning several key performance indicators, including but not limited to the impact on safety, travel times and value for money, equity, spatial accessibility, occupation of public space, and disaggregate impacts on specific populations and zones.

Encourage mobility data sharing protecting individual privacy and commercial sensitivities. Within budgetary constraints, develop, enhance, and expand data sharing frameworks that enable the appropriate processing of data, including open government data, without eroding people's privacy or compromising commercial sensitivities, respecting the principle of data minimisation and identifying a clear link between broad public policy objectives and the type of data collected, its level of aggregation and anonymization, and the rules applied to it regarding its collection, latency, processing, security, permitted uses, storage, retention, and destruction.

Assess and adapt new approaches to leveraging data science to enhance smart mobility data frameworks. Assess new data science developments that could improve smart mobility outcomes, including incorporating novel methods of extracting and sharing reliable information and uncovering and addressing biases in data underpinning smart mobility solutions, as well as encourage public agency or trusted third party data auditing capacity to build trust.

4. Ensure functional interoperability between technologies, infrastructure, and platforms

Encourage interoperability of smart mobility solutions to deliver public value. Encourage interoperability amongst smart mobility services, data architectures, as well as among the technologies that underpin these services at the national and international levels, and work

towards broad compatibility and harmonization of communication networks, including facilitating convergence towards common and shared network solutions through industry-led, voluntary, consensus-based international technical standards for interoperability.

Foster building blocks and interoperability rules supportive of mobility as a service and mobility on demand. Foster basic building blocks for mobility as a service (MaaS) and mobility on demand (MoD) that support a human-centric, inclusive, and sustainable mobility ecosystem, as well as a competitive business environment, such as harmonised and robust digital identifiers, standardized data syntaxes, and open MaaS and MoD platform access rules.

5. Build government digital capacity

Enhance government capacity to process, analyse, and ensure the security of mobility data collected for public purposes. Encourage the integration in education and training of public sector skills to collect, understand, format, clean, parse, and analyse large, unstructured or differently structured and high velocity data, and invest in capacity building so that the public sector develops and retains digital skillsets.

Reinforce local governments' and public transportation agencies' capacities for smart mobility project management in a multi-stakeholder environment. Reinforce public sector capacities and capabilities to assert a leading role in guiding smart mobility, including enhancing local governments' project management and participatory planning capacity, establishing long-term agreements of collaboration and forming inter- and trans-disciplinary working teams.

6. Foster multi-stakeholder collaboration and partnerships

Ensure effective communication, engage with the community, and promote a multi-disciplinary and multi-stakeholder environment for the development of new mobility solutions. Connect with target populations and relevant stakeholders on a regular basis to identify challenges and how they can be addressed, involving businesses, science and technology institutions, and people of different socio-economic backgrounds, gender, age, and marginalized groups, in the development process of smart mobility projects.

Foster collaboration between local, regional, and national governments for the development of smart mobility initiatives, particularly in metropolitan areas. Explore new forms of governance allowing for broader multi-government local, regional, and international partnerships to emerge, especially in metropolitan areas.

7. Develop frameworks to maximize the social value of smart mobility

Adopt frameworks for practices and an environment for smart mobility that fosters transparency, efficiency, competition, and innovation, taking the broader policy environment into account. Establish frameworks for practices that foster and facilitate innovation and avoid increasing the costs of adopting new technology and business models in smart mobility, as well as ensure consumer protection and a competitive business environment and prioritize the development of industry-led, consensus-based, international technical standards to facilitate common regulatory approaches across borders and enhance market access for products and services.

Revise outdated and fragmented smart mobility frameworks. Schedule reviews based on transparent and rigorous methodologies and ensure that mobility data necessary to assess continued fitness-for-purpose frameworks is collected and processed, and make frameworks machine readable where possible.

Annex 3: A G20 Roadmap toward a Common Framework for Measuring the Digital Economy

Accurate and effective measurement of the digital economy is important to enable evidence-based policymaking to help manage the growth opportunities and challenges that the digital economy presents. Thus, following the 2017 *Roadmap for Digitalization* developed under the German Presidency, the 2018 *G20 Toolkit for Measuring the Digital Economy* produced under the Argentine Presidency, and the call for efforts to improve the measurement of the digital economy in 2019 in Japan, in 2020, under the Saudi Presidency, the DETF supported advancing digital economy measurement and enhancing evidence-based policymaking.[3] The Saudi Presidency furthered discussions about measuring the digital economy by promoting a collaborative and multi-stakeholder approach, including conducting a survey to G20 countries and holding a Workshop on measurement of the digital economy, as well as consultation with representatives from the civil society, the private sector, and contributions from regional and International Organizations (IOs)[4].

As a result of this process, under the Saudi Presidency, the DETF has worked to advance toward the development of a common framework for measuring the digital economy. First, building on the outcomes reached in Hangzhou in 2016, the Saudi Presidency has proposed an **overarching policy definition of the different elements of the digital economy**:

"The digital economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services, and data; it refers to all producers and consumers, including government, that are utilising these digital inputs in their economic activities."

The DETF acknowledges that the digital economy has broader societal impacts and therefore, for policy purposes, extends beyond the activity formally recorded in economic statistics. To address this, the overarching policy definition proposed above is combined with a tiered definitional framework to not only assist with accurate measurement and comparability of the digital economy by statistical offices but to also allow for the incorporation of digitalized interactions not currently recorded as economic activity, such as participation in social media or the use of zero-priced digital services.

Second, in 2020 the DETF has recognized the importance of representative indicators related to **Jobs, Skills, and Growth in the Digital Economy**, which seek to complement indicators used to monitor the United Nations 2030 Sustainable Development Goals (SDGs). Representative indicators should have the following characteristics by: (1) collectively address key facets of the Digital Economy, (2) reflect cross-cutting factors such as gender differences, (3) use established definitions, classifications, and sources and (4) take availability with sufficient frequency and country coverage into account. Third, progress was made in discussing and exploring indicators to account for data, digital services, and digital platforms, including public platforms. Finally, with a view to concretize the discussions this year and to establish potential horizons to advance on the measurement of the digital economy, the following "**G20 Roadmap Toward a Common Framework for Measuring the Digital Economy**" sets out potential actions to advance towards a G20 Common Framework for Measuring the Digital Economy.

[3] The background report 'A Roadmap Toward a Common Framework for Measuring the Digital Economy' was produced by the OECD for the G20 Saudi Presidency. The opinions expressed and arguments employed in this report do not necessarily represent the official views of the member countries of the G20.
[4] European Commission, ITU, ILO, IMF, UNCTAD and UNSD.

A G20 Roadmap toward a Common Framework for Measuring the Digital Economy

1. Definitions and concepts

Any measurement framework will need to be founded upon a common definition of elements of the digital economy as well as other key related concepts that complement and operationalize it.

G20 countries are encouraged to consider:

- The definition proposed by the Saudi Presidency in this Roadmap.
- Identifying further elements needed to operationalize the definition which will require further research and discussion.
- Sharing experiences on digital measurement and on operationalizing the definition of the digital economy with G20 countries and beyond.

2. Indicators

To identify the fundamental factors affecting the evolution and development of the Digital Economy, indicators need to be developed, implemented, and monitored. Building on previous DETF work, four measurement pillars have been identified to be included in a G20 common framework that draw on the draft 2018 *G20 Toolkit for Measuring the Digital Economy* put together by Argentina under its Presidency: Infrastructure, Technology Adoption and Innovations, Empowering Society, and Jobs, Skills and Growth. These could be complemented by others as necessary.

G20 countries are encouraged to consider ways to improve indicators used for measuring the digital economy. Inclusion of other relevant stakeholders involved in digital economy measurement work is also important to ensure that indicators reflect and adapt to society's needs.

3. Data and methodologies

The development of sound and comparable indicators will depend on available data sources, data collection strategies, frequency of data collection, methodological developments, and other factors. Sharing best practices and experiences is key in this regard.

G20 countries are encouraged to consider:

- Putting in place foundational infrastructures for collecting relevant data, recognizing internationally accepted standards and practices, in line with their national regulations and priorities.
- Collecting data and leveraging existing data to support key breakdowns of relevant characteristics that are sufficiently robust to be published, possibly including gender, sex, age groups, educational attainment, household income for individuals, and employment size-band and industry for firms.
- Establishing and improving input-output tables.
- Engaging in coordinated international collection mechanisms, where appropriate.

4. Dissemination

Public availability of and reporting on indicators, including in open formats, is critical to allow their use for analysis and policymaking in both national and international contexts.

G20 countries are encouraged to consider:

- Producing and reporting on indicators regularly, as permitted by national circumstances.
- Making the resulting indicators and datasets publicly available, which can contribute to international statistical collections facilitated by IOs.
- Ensuring that key outputs, including reports, indicators, and datasets are available online in accessible formats.

5. Institutional arrangements and capabilities

Institutional capabilities are needed to apply these methodologies and report on indicators regularly and enable the measurement framework to evolve and improve over time by adjusting to emerging policy needs and leveraging new data sources and experience.

G20 countries are encouraged to consider:

- Developing, including through the provision of training, the necessary digital skills that will enable public officials, especially those in National Statistical Offices, to engage in the activities that this Roadmap entails, including the processing and handling of large amounts of data and the use of complementary non-survey data sources and techniques (e.g. web-scraped data).
- Investing in digital infrastructure for statistics, including but not limited to data storage and processing infrastructure and complementary data analysis software.
- Seeking complementary management knowledge and capabilities to engage with relevant stakeholders and explore partnerships that could enhance measurement efforts, including in collaborating with the private sector to explore alternative sources of data and measurement techniques.
- Supporting a multi stakeholder approach, enabling dialogue between relevant stakeholders, including businesses, government, and other actors from civil society, to strengthen the evidence base for measurement of the digital economy.
- Engaging in measurement discussions in multilateral fora and strengthen multilateral collaboration and cooperation to share best practices and experiences and facilitate knowledge transfer.
- Working towards sharing experiences and best practices between G20 countries.

Annex 4: G20 Examples of Practices Related to Security in the Digital Economy

The purpose of these G20 Examples of Practices Related to Security in the Digital Economy is to provide countries with examples of national and local efforts to support organizations in enhancing their security in the digital economy, some of which can be utilized by MSMEs. The examples in this list are drawn exclusively from submissions provided by G20 member states and guest countries to the Saudi G20 Presidency. This list is non-exhaustive, is not prescriptive in any way, and inclusion on this list does not reflect endorsement by G20 members. Among the wide variety of possible practices that support Security in the Digital Economy, G20 members and guest countries provided the following list of examples (wherever available, a link is included to the source document, as provided by the G20 or Guest Country):

- **National Strategies and Plans:** 2016 Cyber Security Strategy: Enabling Innovation, Growth & Prosperity (Australia); National Cybersecurity Strategy 2020 (Brazil); National Cyber Security Strategy (Canada); National Cyber Security Action Plan (Canada); Internet Plus Action Plan (Internet Plus) (China); French National Digital Security Strategy (France); Cyber Security Strategy for Germany (Germany); Cybersecurity Technology Roadmap 2020-2045 (Indonesia); National Cyber Security Strategy (Italy); Italian Cyber Security Action Plan (Italy); Cybersecurity Policy for Critical Infrastructure Protection (Japan); Cybersecurity Strategy (Japan); National Cybersecurity Strategy (Republic of Korea); National Digital Strategy (Mexico); National Development Plan (NDP) 2019-2024 (Mexico); "Internet for Everyone" Program (Mexico); "Digital Economy" National Program (Russian Federation); Saudi National Cybersecurity Strategy (Saudi Arabia); Singapore's Cybersecurity Strategy (Singapore); National Strategy for the Protection of Switzerland Against Cyber Risks 2018-2022 (Switzerland); 2016-2019 National Cyber Security Strategy (Turkey), National Cyber Security Strategy 2016-2021 (United Kingdom); National Cyber Strategy of the United States 2018 (United States)

- **National Agencies, Centers, and Institutes:** Australian Cyber Security Centre (ACSC) (Australia); Canadian Centre for Cyber Security (Canada); National Cybercrime Coordination Unit (Canada); Spam Reporting Centre (Canada); Canadian Anti-Fraud Centre (Canada); European Union Agency for Cybersecurity (ENISA) (EU); National Cybersecurity Agency of France (ANSSI) (France); Federal Office for Information Security (Germany); National Cyber and Crypto Agency (Indonesia); National Center for Incident Readiness and Strategy for Cybersecurity (NISC) (Japan); Government Security Operation Coordination team (GSOC) (Japan); Korea Internet & Security Agency (KISA) (Republic of Korea); National Association for International Information Security (Russian Federation); AMO Analytical Agency for Computer Security (Russian Federation); National Cybersecurity Authority (NCA) (Saudi Arabia); National Risk Assessment Function (e-NRAF) (Saudi Arabia); Cyber Security Agency of Singapore (Singapore); Spanish National Cybersecurity Institute (INCIBE) (Spain); Spanish Agency of Data Protection (AEPD) (Spain); National Cyber Security Center (NCSC) (Switzerland); Presidency of the Republic of Turkey Digital Transformation Office (Turkey); Personal Data Protection Authority (Turkey); Information and Communication Technologies Authority (Turkey); Ministry of Industry and Technology – The Scientific and Technological Research Council of Turkey Informatics and Information Security Research Center (TUBITAK BILGEM) Cyber Security Institute (Turkey); National Crime Agency (United Kingdom); National Cyber Security Centre (NCSC) (United Kingdom); Cyber Crime Reporting Centre (United Kingdom); Cybersecurity and Infrastructure Security Agency (CISA) (United States)

- **Policies, Frameworks, and Schemes:** Cyber Secure Canada (Canada); National Cyber Security Horizontal Initiative Framework (Canada); National Cyber Security Policy (India); Preferred Market Access (PMA) Policy for Cyber Security Products (India); Presidential Regulation No. 74 of 2017 regarding E-Commerce Roadmap (Indonesia); National Framework of Cybersecurity and Data Protection v. 2.0 (Italy); General

Framework for Secure IoT Systems (Japan); Information Security Master Plan for the Private Sector (2019) (Republic of Korea); National Cybersecurity Incident Response Framework (NCIR) (Saudi Arabia); National Cybersecurity Information Sharing Framework (NCISF) (Saudi Arabia); Risk Management Framework (RMF) (Saudi Arabia); Risk Process Management System (RPMS) (Saudi Arabia); Risk Management and Assessment (RMA) (Saudi Arabia); SAMA Cyber Security Framework (Saudi Arabia); Saudi Cybersecurity Workforce Framework (SCyWF) (Saudi Arabia); Cybersecurity Labelling Scheme (Singapore); The National Cybersecurity Policy Framework for South Africa (NCPF) (South Africa); Information and Communication Security Measures Decree No. 2019/12 (Turkey); Cyber Assessment Framework (CAF) (United Kingdom); Cyber Essentials (United Kingdom); NIST Cybersecurity Framework (United States)

- **National Laws and Regulations:** Cybercrime Law 26.388 (Argentina); Digital Signature Law 25.506, with associated Decree No.2628/2002 (Argentina); Personal Data Protection Law 25.326, and Decree No. 1558/2001 (Argentina); National Law No. 27.483 (Argentina); Modernized Convention 108 (Argentina); General Personal Data Protection Law (LGPD) (Brazil); Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada); Breach of Security Safeguards Regulations (Canada); Canada's Anti-Spam Legislation (Canada); Cyber Security Law of the People's Republic of China (Internet Security Law) (China); Cybersecurity Act (EU); General Data Protection Regulatory (GDPR) (EU); (Network and Information System) NIS Directive (EU); IT Security Law (Germany); Information Technology Act, 2000 (India); Government Regulation No. 80 of 2019 regarding Electronic Trading System and Indonesian General Data Protection Regulatory (GDPR) (Indonesia); Act no. 19 of 2006 on the Revision of the Act no. 11 of 2008 on Electronic Information and Transaction (UU ITE) (Indonesia); CIIP Law (France); Legislative Decree 65/2018 on the Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Italy); Parliamentary law 133/2019, National Cybersecurity Perimeter (Italy); Act on the Protection of Personal Information (APPI) (Japan); Basic Act on Cybersecurity (Japan); Electronic Signature Law (2012) (Mexico); Federal Law on Protection of Personal Data by Private Parties (Mexico); Act on the Promotion of Information and Communication Network Utilization and Information Protection, etc. (Republic of Korea); Act on the Protection of Information and Communications Infrastructure (Republic of Korea); Personal Information Protection Act (PIPA) (Republic of Korea); Saudi Anti-Cyber Crime Law (Saudi Arabia); Cybersecurity Act (Singapore); Protection of Personal Information Act (South Africa); Law on the Protection of Personal Data (Turkey); By-Law On Data Controllers Registry (Turkey); By-Law on Erasure, Destruction or Anonymization of Personal Data (Turkey); Electronic Communications Law No. 5809 (Turkey); Regulation on Network and Information Security in Electronic Communications Sector (Turkey); Computer Misuse Act 1990 (United Kingdom); Network and Information Systems Regulation 2018 (United Kingdom); Regulatory of Investigatory Powers Act 2000 (United Kingdom); UK Code of Practice for Consumer IoT Security (United Kingdom); Online Harms White Paper (United Kingdom); The Data Protection Act, 1998 (United Kingdom); Data Protection Act 2018 (United Kingdom); The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (United Kingdom); Section 7 of the Electronic Communications Act (United Kingdom); The Data Protection (Charges And Information) Regulations 2018 (United Kingdom)

- **Standards and Controls:** Complementary Standard on Security Risk Management Methodology (Brazil); Complementary Standard on Information Security Risk Management (Brazil); Baseline Cyber Security Controls for Small and Medium Organizations (Canada); EBIOS Risk Manager (EBIOS) (France); IT-Grundschutz (Germany); BSSN IT Security Assessment and Audit (Indonesia); Common Standards

on Information Security Measures of Government Entities (Japan); Personal Information & Information Security Management System (Republic of Korea); Cybersecurity Code of Practice for Critical Information Infrastructure (Singapore); Essential Cybersecurity Controls (ECC-1: 2018) (Saudi Arabia); Cybersecurity Controls for Remote Work during the COVID-19 Epidemic Response (Saudi Arabia)

- **CERTs, CSIRTs, and Support Services:** ACSC's ReportCyber (online cybercrime reporting platform) (Australia); CERT.br and CTIR.gov.br (Brazil); CERT-EU (EU); Cybersecurity of 5G Networks (EU); Cybermalveillance.gouv.fr (France); Security Visas (France); Indian Computer Emergency Response Team (CERT-In) (India); National Computer Security Incident Response Team (Indonesia); BSSN's Cyber Incident Helpline Service (Indonesia); Cyber Security Incident Response Team CSRIT-Italia (Italy) "NOTICE" (National Operation Towards IoT Clean Environment) project (Japan); CERT-MX (Mexico); Korea Internet Security Center (KrCERT/CC) (Republic of Korea); IOT Security Certification and IOT Security Test Bed (Republic of Korea); Information security consulting for local MSMEs (Republic of Korea); DDoS Shelter (Republic of Korea); Vulnerability Analysis and Evaluation (Republic of Korea); Protection of the Rights and Legitimate Interests of Business in the Digital Economy (Russian Federation); National Computer Incident Response and Coordination Center (Russian Federation); Saudi CERT (Saudi Arabia); SingCERT (Singapore); Cybersecurity Hub (South Africa); Helpline "Free Help Line (017): Cybersecurity" (Spain); National Cyber Security Incident Response Team (TR-CERT) (Turkey); National Cyber Security Center (NCSC) (United Kingdom); Active Cyber Defence (United Kingdom); CiSP (Cyber Security Information Sharing Partnership) (United Kingdom); Cybersecurity and Infrastructure Security Agency (includes the former US-CERT) (United States)

- **Capacity-Building Programs and Resources:** SME Technical Assistance Program (initial phases, not yet implemented) (Argentina); Digital Security Startup Programs and Accelerators (Brazil); ASSEMBLYLINE (Canada); Harmonized Threat & Risk Assessment Model (Canada); Cyber Security Cooperation Program (Canada); Cybertitan (Canada); ANSSI Toolkit to Strengthen the Security of Personal Data (France); IT Security in Commerce (Germany); National Cybersecurity Program (India); Grand Challenge on Cyber Security (India); Information Security Education and Awareness (ISEA) project (India); CyberShikshaa (India); Cybersafe India (India); Cyber Safety India (CSB) Programme (India); BSSN Human Resource Development on Awareness, Training, and Consultation (Indonesia); Digital Talent Scholarship on Cybersecurity (Indonesia); Information Security Self-Assessment for MSMEs (Indonesia); Cyber Risk Self-Assessment Project (Italy); Cybersecurity Supporters for SMEs (Japan); MSMEs Grants for Adoption of ICT Technologies (Japan); Cyber Security Training & Certification Center (KISA) (Republic of Korea); WHISTL (Republic of Korea); CASTLE (Republic of Korea); Federal Project "Information Security" (Russian Federation); Cybersecurity Toolkit (Saudi Arabia); ASEAN-Singapore Cybersecurity Centre of Excellence (Singapore); Facilita RGPD (Spain); "Capture-the-Flag" competitions (Turkey); Turkish Cyber Security Cluster Innovation Competitions (Turkey); Cyber Security Training Portal (Turkey); Cyber Security Body of Knowledge (CyBOK) (United Kingdom); The London Cyber Innovation Centre (United Kingdom); Cyber 101: Business Skills Bootcamps for Cyber Security SMEs (United Kingdom); Financial support for academic start-ups in cybersecurity (United Kingdom); Enhanced tax relief and vouchers for cybersecurity investment (United Kingdom); The ACE and PhD programmes (United Kingdom); Cheltenham Innovation Centre (incl. the Cyber Accelerator) (United Kingdom); CyberFirst (United Kingdom); Exercise in a Box (United Kingdom); Board Toolkit (United Kingdom)

- **Knowledge Resources:** Implementation of the Principles of Security in Cloud Guide (Argentina); Small Business Cyber Security Guide (Australia); ACSC Small Business

Survey Report (Australia); Step-by-Step Guide Automatic Updates (Australia); Step-by-Step Guide Backing up and Restoring your Files (Australia); Step-by-Step Guide Turning on Two Factor Authentication (Australia); Quick Wins for your Portable Devices (Australia); Quick Wins for your Website (Australia); Get Cyber Safe (Canada); Canadian Centre for Cyber Security Publications (Canada); Information Security and Privacy Standards for SMEs (EU); Guidelines for SMEs on the Security of Personal Data Processing (EU); Charter for the Use of IT and Digital Resources (France); Digital Risk Management Guide (France); Information Guide on Good Practices (France); Information System Hygiene Guide (France); Controlling Digital Risk - The Trust Advantage (France); Awareness Guide (France); Practical Guidelines and Simplifying Measures for SMEs (Italy); CISO Roles and Responsibilities (India); CISOs Top 10 Best Practices Guidelines (India); General Guidelines for Secure Applications and Infrastructure (India); Information Security Management System (ISMS) (India); Checklist for Secure Code Programming in Application (India); Guidelines on Cyber Security Management during Covid-19 Pandemic (Indonesia); Telework Security Guidelines (4th Edition) (Japan); Guidance on Responding to Denial of Service Attack (for MSMEs) (Republic of Korea); Ransomware Response Guide (Feb 2018) (Republic of Korea); Security Guide on Introducing and Operating a Remote Working Environment (Republic of Korea); E-commerce Cybersecurity Guidelines for Service Providers (Saudi Arabia); Be Safe Online (Singapore); SME Go Digital (Singapore); Protect Your Business (Spain); Home Office: End User Guideline (Switzerland); Home Office: Securing Remote Access (Switzerland); Information Security Checklist for SMEs (Switzerland); Instructions for Cleaning Up Websites (Switzerland); Measures to Counter DDoS Attacks (Switzerland); Information and Communication Security Guide (Turkey); Institutional and Sectoral CERTs Establishment and Management Guides (Turkey); Cybersecurity Precautions Measurement Test for Institutions (Turkey); Minimum Security Precautions for Information Systems in Critical Infrastructure (Turkey); NCSC's Small Business Guide (United Kingdom).