

From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows

WHITE PAPER

APRIL 2023

Contents

Foreword	3
Executive summary	4
1 Introduction	5
1.1 The historical backdrop	5
1.2 The need for an institutional mechanism	6
1.3 Purpose of this white paper	7
2 Importance of the free flow of data	8
2.1 Trends and changes in the global context since the DFFT proposal	8
2.2 The significance of data flows for the global economy	8
3 Headwinds facing the free flow of data	11
3.1 Uncoordinated domestic regulation	11
3.2 The impact of regulatory fragmentation	14
3.3 Interoperability to address regulatory fragmentation	16
4 The opportunity to institutionalize DFFT	17
4.1 Challenges for regulatory interoperability	17
4.2 New momentum to collaborate on cross-border data flows	18
4.3 The unique potential of a new institutional mechanism	18
5 Conclusion	21
Contributors	22
Endnotes	24

Disclaimer

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

© 2023 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Foreword



Helena Leurent
Managing Director,
Consumers International



Bob Hedges
Chief Data Officer, Visa



Jeremy Jurgens
Managing Director,
World Economic Forum

Digital transformation has the potential to uplift economies and enable people, businesses and societies to thrive. Data flows power the digital economy, creating a flywheel for growth and inclusion. To realize the full potential of the digital economy, however, data must flow across borders. Multilateral, international and public-private cooperation is, now more than ever, essential to address global data policy challenges. Ensuring that data flows efficiently and responsibly across borders requires addressing privacy, online safety, disinformation and other concerns. Ensuring the free flow of data across borders while securing trust is an urgent priority for people, businesses, governments and institutions. Improving coordination can enable more informed choices and better delivery of solutions for people and our planet.

The time to act is now. The movement of data across country borders is essential to global and local economies, carrying information and enabling innovation, economic value and wealth. To put it in perspective, the data transfer relationship between the United States (US) and Europe alone is worth about \$7.1 trillion.¹ International trade underpinned by data flows reached nearly \$700 billion in exports from the US and nearly \$500 billion in imports.² As a result of data flows between the European Union and US, businesses in Europe have access to a market of over 300 million new users and US businesses have access to a market of 450 million. Data access and sharing across borders may generate social and economic benefits of up to 2.5% of gross domestic product (GDP).³

Multistakeholder dialogue and international cooperation to augment the value of cross-border data flows is also key to pursuing and successfully addressing a range of global challenges ranging from inclusive finance to healthcare to global supply chains. Global data transfers enable an array of essential activities, including multi-country clinical

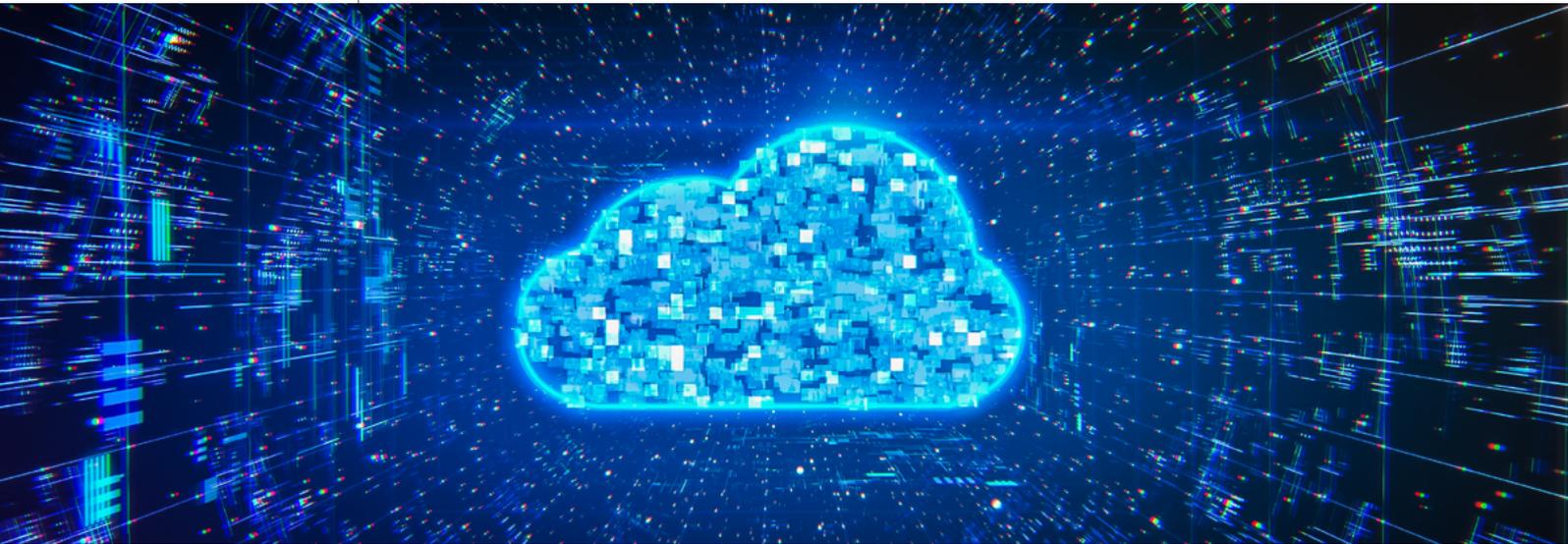
trials, cybersecurity threat information sharing, and anti-fraud and anti-money laundering efforts. The free flow of data across borders can provide decision-makers with critical information needed to achieve global objectives such as the Sustainable Development Goals and to navigate the complex economic, social and financial crises facing our world today.

In 2019, the late Japanese prime minister Shinzo Abe declared the launch of “Data Free Flow with Trust (DFFT)”, a model for establishing a trust framework for cross-border data flows. Since then, DFFT has been endorsed in various international forums, including the Group of Seven (G7) and Group of Twenty (G20). In 2022, the World Economic Forum mobilized a multistakeholder DFFT task force to develop policy recommendations to advance interoperability between existing regulatory approaches.

The year 2023 marks an important milestone in the journey towards operationalizing DFFT. With the Government of Japan holding the G7 presidency and championing the cross-border data flows agenda, a significant opportunity exists for the global multistakeholder community to advance a common framework for establishing an institutional mechanism for cross-border data flows. Such a mechanism would facilitate the required digital policy coordination across governments, private sector, non-governmental organizations and civil society to put the DFFT concept into practice and advance cooperation on issues such as data privacy, cybersecurity, user consent and data transfers.

This white paper endorses a trusted policy coordination mechanism for cross-border data flows to fully operationalize DFFT and unlock the value of data for the benefit of our world. With the right institutional mechanism, the DFFT concept could facilitate economic growth and help unlock the value of strong and enduring cross-border data flows.

Executive summary



Digitalization has transformed the global economy and society, bringing markets and people closer together. Data, and the ability to move it seamlessly across borders, have become critical for the digital economy. Yet there are few effective and trusted policy coordination mechanisms to support cross-border data flows. Filling this gap is key to unlocking global economic growth and sustainable development. In this context, the “Data Free Flow with Trust (DFFT)” concept announced in 2019 offers a framework for the protection of sensitive data and for secure data transfers across borders.

The objective of this paper is to highlight the importance of an institutional mechanism to promote cross-border data flows and urge world leaders in the public and private sectors to take collective action towards establishing such a mechanism.

Based on a review of existing research and an assessment of the existing regulatory landscape, this paper finds that:

- Cross-border data flows are fundamental to the economy and society.
- Data flows that are anchored in trust should benefit all stakeholders, from individuals and small and medium enterprises (SMEs) in emerging markets to governments and businesses around the world.
- Despite the benefits, the global data policy landscape is becoming increasingly complex; increasingly fragmented regulations can increase costs for businesses, disempower individuals, deter innovation and curb economic growth.

- Trade agreements and recognition of foreign laws and regulations are two existing mechanisms to remove unnecessary restrictions and increase interoperability for the free flow of data, though their current use remains limited.
- A global data policy environment that supports interoperability while maintaining national regulatory discretion would help minimize fragmentation. In this context, there is growing interest in operationalizing DFFT through an institutional mechanism involving different stakeholders, both governmental and private.

This white paper concludes with a discussion on how an institutional mechanism can help operationalize DFFT and promote cross-border data flows. It recommends that governments starting with the Group of Seven (G7) member-countries’ aim for a permanent new institutional mechanism to complement the work of existing international forums. The proposed mechanism would convene senior government officials and high-level representatives of multiple stakeholder groups. It would be empowered to test new ideas and practical steps to increase interoperability.

An institutional mechanism can go beyond the search for short-term fixes and catalyse long-term thinking for sustainable solutions to operationalize DFFT, advance the global digital economy, and support the economic growth and general welfare of all.

1

Introduction

1.1 The historical backdrop

Digitalization has transformed the global economy and society, bringing markets and people closer. Data has become one of the most critical elements of the digital economy,⁴ and the ability to move data across borders seamlessly and securely for the benefit of everyone is becoming increasingly vital for the global community – whether for promoting economic growth, improving public services or advancing scientific research. The importance of cross-border data flows will continue to grow as emerging technologies such as artificial intelligence (AI), metaverse, blockchain and internet of things (IoT) continue to develop and spread.

Policy-makers are looking for ways to support the digital transformation – and the benefits it brings – while protecting public interest and advancing specific public policy goals. Finding the right balance is difficult, and, unfortunately, domestic rules governing data are becoming increasingly fragmented, restrictive and often disruptive for trade and other economic activities. Although avowedly premised on privacy, security, transparency and similar policy considerations, these rules may in some cases be motivated by other policy goals to advance broader domestic agendas. However, a relative

lack of coordination among governments and a gradual erosion of trust among stakeholders in these data ecosystems has led to increasing regulatory fragmentation. The World Economic Forum's multistakeholder expert group has recognized the absence of effective and trusted policy cooperation mechanisms to support cross-border data flows.⁵

To address this challenge, at the 2019 World Economic Forum Annual Meeting in Davos-Klosters, the Japanese prime minister at the time, Shinzo Abe, introduced the concept of "Data Free Flow with Trust (DFFT)" as a principle to ensure the protection of sensitive data and the secure transfer of data across borders.⁶

In June of the same year, trade and digital economy ministers at the Group of Twenty (G20) ministerial meeting in Tsukuba, Japan, highlighted the significance of cross-border data flows for productivity, innovation and sustainable development, and emphasized the need to address challenges such as security, data protection and intellectual property rights that influence public trust in digital technologies.⁷ The concept has since found support at major global forums including the G20 and G7 (see Box 1).

BOX 1 Growing support on the DFFT concept

- At the G20 Osaka summit, heads of government agreed to work towards the DFFT vision – the leaders' declaration stated that legal frameworks regarding cross-border data flows, both domestic and international, should be respected and, at the same time, the interoperability between each framework must be enhanced to allow data to flow more freely.⁸ The world leaders also recognized the value of the Osaka Track which Japan sought to frame as a collective term for the global governance processes being implemented to unleash the benefits of more open and trusted data flows.
- During the 2021 G7 summit under the United Kingdom (UK) presidency, G7 leaders endorsed a "Roadmap for Cooperation on Data Free Flow with Trust" to better leverage the potential of data-driven technologies while continuing to address data protection challenges. The G7 DFFT roadmap sets out a "plan for delivering tangible progress on this agenda, building confidence for businesses and individuals to use technology, as well as driving economic and social value".⁹
- Subsequently, at the 2022 G7 summit under the German presidency, the leaders adopted a "G7 Action Plan for Promoting Data Free Flow with Trust" to further work on this topic.¹⁰ In parallel, the G20, which has a broader membership encompassing developing countries, also endorsed DFFT. At the latest G20 summit in Bali, the leaders' declaration clearly stated that they "remain committed to further enable data free flow with trust and promote cross-border data flows."¹¹
- In addition to the G7 and G20, the Organisation for Economic Co-operation and Development (OECD) has long recognized the role that both cross-border data flows and trust play in the digital economy.¹² Further, the 21 economies of the Asia-Pacific Economic Cooperation (APEC) forum, a group that includes developing countries, noted in its 2020 leaders' declaration that member countries "acknowledge the importance of cooperation in facilitating the flow of data and strengthening consumer and business trust in digital transactions."¹³

Building upon this history of discussions in international forums, the Japanese government has been leading the global discussion to operationalize DFFT in the run-up to the G7 summit in 2023. At the G20 digital economy ministers' meeting in 2022, the Japanese government noted that DFFT "requires the methods to enhance interoperability across the different ways of data governance, and transparency of regulations" and added that "Japan will also establish an international institutional arrangement to promote a new governance utilizing advanced technologies such as PETs (Privacy-Enhancing Technologies)".¹⁴

Japanese officials have continued to promote the DFFT concept at international conferences, noting that Japan will take the opportunity during the 2023 G7 summit to create consensus to accelerate institutional cooperation and technological responses to DFFT. They will propose an international framework for public-private partnerships, called the "Institutional Arrangement for Partnership (IAP)", that will serve as the core of this effort.¹⁵



1.2 The need for an institutional mechanism

As digital economic activity continues to expand, many countries are putting forward regulatory frameworks related to data privacy, national security and intellectual property, or for economic reasons such as protecting domestic jobs. A recent OECD report shows that a growing number of countries are adopting data localization rules, explicitly requiring that data be stored and/or processed within their territory. Data localization measures are also becoming more restrictive: in 2021, two-thirds of such measures involved both storage requirements and flow prohibitions.¹⁶ Unfortunately, these data localization requirements can impact data flows and have broad economic consequences by creating regulatory fragmentation, hindering cross-border data sharing, harming innovation, raising costs for users and hampering economic growth. Such data localization requirements may also undermine many of the

intended policy objectives including cybersecurity, fraud prevention, financial transparency, regulatory compliance and digital inclusion.

Cybersecurity provides an illustrative example: unobstructed data flows are critical to cybersecurity – and sector-specific objectives like payment fraud disruption capabilities – to monitor traffic patterns, identify anomalies and divert potential threats. Additionally, companies may choose to store data at geographically diverse locations to reduce the risk of physical attacks and to enable companies to reduce network latency, as part of a comprehensive strategy to maintain cyber and operational resilience. When governments mandate localization or restrict the ability to transfer and analyse data in real-time, they may introduce unintended risk by handicapping more comprehensive mitigation techniques. The reality is that digital commerce

is global; so too are bad actors – they are not confined by physical borders. In order to properly guard against them, data shouldn't be either.

Although trust rests on privacy, transparency, accountability, security and personal data protection, the rules need not be designed in a manner that hinders the free flow of data. At the same time, given how public interest in safeguarding privacy and sensitive national security and financial data can be defined differently from country to country, it is unrealistic to believe that governments will move to harmonize their approaches to cross-border transfer of data by delegating the development of standards to an international body. To pursue the desired regulatory interoperability for data transfer and sharing, different countries would need to embrace and use compatible standards and protocols for their key digital and data management processes. A data

policy environment that supports interoperability and maintains national regulatory discretion would minimize fragmentation.

To pursue and ensure regulatory interoperability, it is essential to have an institutional mechanism that brings together government officials, and also experts from international organizations, businesses, civil society, academia and other stakeholders to discuss critical issues. Such an institutional mechanism could also provide the global system with the additional agility needed to keep pace with a rapidly evolving digital economy. This is in line with the recent works from the World Bank and the United Nations Conference on Trade and Development (UNCTAD) that also point to the need for a global framework or body to coordinate the governance of data with the participation of all stakeholders.¹⁷

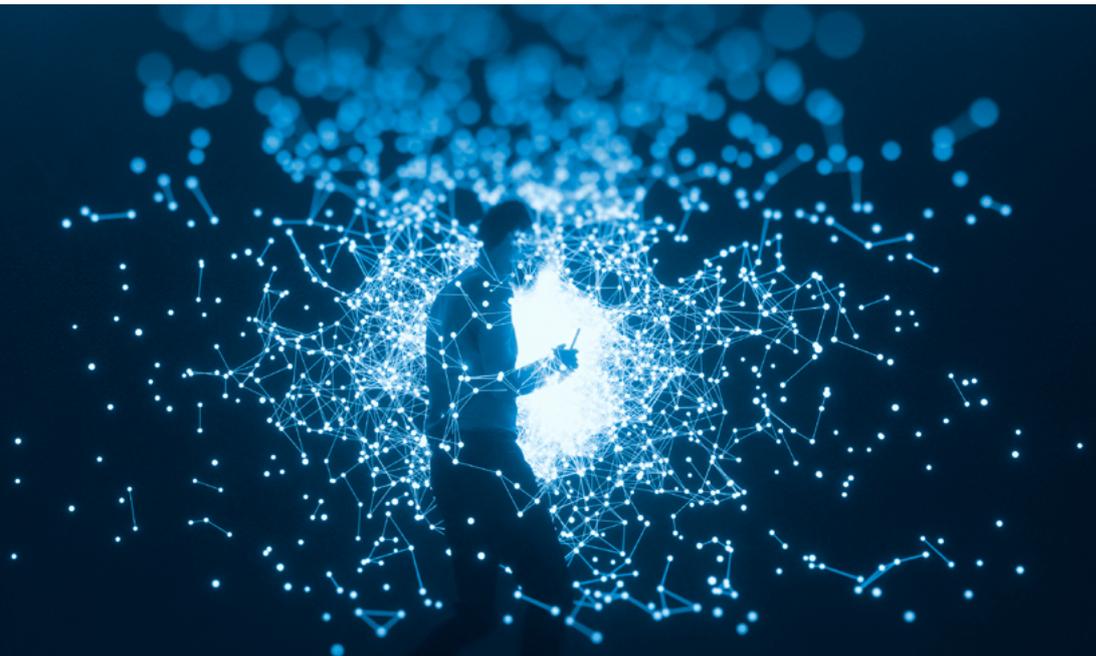
1.3 The purpose of this white paper

Even as the centrality of cross-border data flows to the economy and society is clear, experience has shown that regulatory interoperability can resolve regulatory fragmentation. Globally, there is growing interest in operationalizing DFFT through an institutional mechanism involving different stakeholders, both governmental and private.

In support of operationalizing DFFT, this white paper seeks to:

- Review the progress on cross-border data flows in recent years.

- Highlight the importance and value of an institutional mechanism to promote cross-border data flows.
- Address why the establishment of an institutional mechanism now is central to fully realizing the gains from cross-border data flows.
- Make the case for the benefits of an institutional mechanism to advance DFFT.
- Urge world leaders in the public and private sectors to take collective action towards the establishment of such an institutional mechanism.



2

The importance of the free flow of data

2.1 Trends and changes in the global context since the DFFT proposal

The continuing rise of global data flows and digital trade

Global data traffic reached 230 exabytes, or 230 billion gigabytes, per month in 2020 and is expected to more than triple to 780 exabytes per month by 2026.¹⁸

Technological developments are continuing to power the digital revolution; internet connectivity and ever-expanding computing power have led to a rapid increase in data production and processing that has profoundly impacted the production, consumption and trade of goods and services. These powerful forces continue to drive the evolution towards a data-driven economy and to increase the importance of digital trade. One study shows that by 2023, cross-border business-to-business commerce could account for two-thirds of digital trade (\$1.78 trillion).¹⁹ In the US alone, international trade underpinned by data flows reached nearly \$700 billion in exports and \$500 billion in imports in 2018.²⁰ It is also estimated that 70% of new value created in the economy over the next decade will be based on digitally enabled platform business models.²¹

The impact of the COVID-19 pandemic

The pandemic significantly accelerated the digitalization trend, by making a profound impact on everything from the way users buy goods to the way businesses conduct meetings. Although e-commerce was growing at a rapid pace already, the pandemic fundamentally changed the way users interact with the world. During the pandemic's early days, the OECD recognized this shift, noting that the health crisis significantly accelerated the digitalization trend.²² Globally, most businesses faced an ample decrease in revenues – for instance, airline revenues dropped about 60% in 2020. However, technology companies such as Apple, Google, Microsoft and Samsung achieved a rise in revenues during the same period through digital trade. Users became accustomed to shopping online, and e-commerce grew significantly.²³ According to the OECD, between May 2019 and May 2020, online orders increased by 50% in Europe and 120% in North America.²⁴ As the world continues to recover from the global pandemic, it is increasingly clear that the digitalization trend is here to stay.

2.2 The significance of data flows for the global economy

Contribution to innovation and economic growth across all sectors

Strategic investments in digital technologies can have wide-ranging economic benefits. In general, digital technologies encourage economic activity through reduced search and information costs, making the global market accessible to buyers and sellers from all parts of the world. Businesses are increasingly incorporating data-

intensive technologies in core business processes, making data flows vital to the competitiveness of firms in virtually every industry. As a result, many governments are updating trade policies to promote participation in the data-driven economy. This represents a shift in focus from the 1990s and 2000s, when “the digital economy” considerations were largely conceptualized as sector-specific provisions for the Information and Communications Technology (ICT) industries. Today, policy-makers recognize that data-flows are not limited to the

ICT sector. On the contrary, digital capabilities are integral to the business models of firms engaged in manufacturing activities, too, where data is pervasive in all stages of design, production, delivery and use.²⁵

According to one study, data access and sharing across borders may generate social and economic benefits of up to 2.5% of GDP, and broad adoption of open-data ecosystems could yield benefits of up to 1.5% of GDP in 2030 in the EU, UK and US, and as much as 5% in India.²⁶

A *Harvard Business Review* study in 2020 showed that the economies that thrived the most were open to digital trade and did not impede data flows.²⁷ The study also clearly showed that open data flow was achievable even while allowing for strong consumer privacy protection, and cited Canada, Japan, the Netherlands and Singapore as examples.

Impact on small and medium enterprises

Perhaps no group has been more impacted by these changes than small and medium enterprises (SMEs), which need cross-border data flows for better and faster access to critical knowledge and information so as to overcome information disadvantages vis-à-vis larger firms.²⁸ A 2021 survey of US-based small businesses found that the pandemic brought both challenges and opportunities for SMEs.²⁹ While a large percentage of the firms surveyed experienced revenue declines, those that were digitally enabled tended to fare better. Businesses that leveraged digital tools and online marketplaces proved to have greater resiliency and agility, and those with an online presence were able to expand sales volumes



and international reach. Surveys of SMEs in other markets including Dubai and the UK found similar results.³⁰ In general, digitalization was instrumental in both helping companies make it through the pandemic as well as expand into new markets.

Focusing on women-led small businesses, another recent study suggests that greater access to digital tools for women supports enhanced financial inclusion and contributes to economic growth.³¹ Specifically, the paper looked at the impact of the COVID-19 pandemic on a group of women

entrepreneurs in Bangladesh and found that those that digitalized were able to expand beyond their domestic market, opening up opportunities in Australia, Canada, Italy and the US. On average, the women increased business leads totalling \$119,000, and supported other women-led domestic suppliers, sourcing from 14 new women-owned suppliers on average.

More broadly, cross-border data flows along with digital technologies allow SMEs to compete with larger firms by lowering barriers to entry, reducing costs and increasing efficiency. SMEs can leverage digital platforms, cloud computing, storage and software without the need for significant upfront investments in information technology (IT) infrastructure. This cost-effective access to technology and other online tools allows SMEs to scale their operations, improve efficiency and compete with larger players in their respective industries in the global market.

Impact on developing countries

Cross-border data transfers are critical to facilitate developing countries' access to global markets, innovation, finance, food and healthcare.

For instance, in the context of providing finance to SMEs in developing countries, digital financial services such as mobile banking, digital payment platforms, crowdfunding and investment platforms, as well as online lending platforms, can offer more affordable and accessible financial products.

A World Bank report highlights the benefits of cross-border data flows from the perspective of individuals living in developing countries.³² It cites the case where a Bangladeshi firm, Augmedix, offers remote assistance to medical doctors in the US. In this case, the doctors wear smart glasses allowing their Bangladesh-based assistants to "witness" patient consultations and create associated medical records. This two-way exchange of data across borders and the associated high value-added services shows that cross-border data flows could create concrete benefits for individuals living in developing countries.

Of course, securing further cross-border data flows is not a silver bullet for addressing all digital issues in developing countries. To harness the power of data and reap the benefits of data and cross-border data flows, developing countries will have to address not only the operationalization of DFFT but also wider digital issues, such as enhancing digital skills among their people, building trusted and equitable mechanisms for transparency, accountability, online safety and access, and removing bias and disinformation. In this way, developing countries could create a more inclusive and ethical digital environment for the benefit of all.

Impact on users

User adoption of digital technologies will have lasting effects across many different sectors of the economy. Before the pandemic, sectors such as education and healthcare were largely local, constrained by the need to physically be in classrooms or doctors' offices. Online classes and teleconsultations have fundamentally changed the way users consume certain services. According to McKinsey, these changes will last. In a 2021 survey, it found that users were increasingly tech-savvy and had learned to access a wide variety of services by digital means, such that "once exposed to best-in-class experiences and offerings across industries and around the globe, ever more digitally savvy users may be reluctant to settle for less."³³

As users continue using digital technologies, they will increasingly share more data, making it important to empower them to make informed decisions about what data they share, for what purpose and with whom. According to Visa research, empowering consumers with control and choices will result in more trusting and confident digital consumers.³⁴ Consumer confidence in data sharing is fundamental to the continuing growth of global data flows.

Cross-border data flows have a significant impact not only on the services people use but also on the physical devices they use or own. For example, vehicles with over-the-air update capability allow auto manufacturers to address energy efficiency, safety and other performance issues via satellite and cloud-enabled software updates. Similarly, sensors throughout the vehicle allow for on-the-road monitoring and predictive maintenance via cross-border cloud-enabled technologies.³⁵

Unlocking the power of data can also help overcome barriers to access, creating a more inclusive and equitable digital economy. Billions of people worldwide (including 28 million in the US and 5 million in the UK) lack a documented credit history, which means they are not viewed as being creditworthy by traditional standards.³⁶ An innovative application of data makes it possible for financial institutions to make more holistic and appropriate underwriting decisions by analysing consumers' complete payment patterns.

The trend towards open finance is enabling a more connected view of underbanked users' financial activities, which can improve their creditworthiness. As national authorities make progress towards greater openness, however, the lack of coordination at the international level could result in divergences that widen access gaps.

Headwinds facing the free flow of data

3.1 Uncoordinated domestic regulation

While the digital economy has clear benefits, its expansion brings challenges too. Governments are increasingly trying to facilitate open data flows and innovation while protecting the public interest on issues such as data privacy, consumer data rights and cybersecurity. Developing the right regulatory balance can be especially difficult when technological change is advancing rapidly. Contributing to this complexity, government motivations for implementing regulatory requirements differ across jurisdictions. As a result, new regulatory requirements are increasing both at a significant rate and with varying complexity. For example, research shows that new data governance rules have been proposed every day so far this year by Europe, the G20 and Switzerland.³⁷

Many of these new regulatory requirements are focused on some form of data localization. While data localization laws may be well intended – to protect consumer privacy, guard against cyber breaches, or advance the digital economy – they can also impede economic growth by raising technological and operating costs and curtailing innovation. The sought-after consumer or public benefits of data localization can get eroded by unintended but deleterious economic side-effects. Data localization can also have negative societal implications. In the context of the global fight against crimes, data localization laws that undercut the ability to develop a clear picture of global criminal operations can thwart efforts to curb nefarious activities such as money-laundering, terror financing and human and wildlife trafficking. At the same time, the proliferation of fragmented rules across markets increases regulatory uncertainty, further increasing costs, efforts and time for businesses, particularly SMEs.

Data localization laws are on the rise

Local storage requirements continue to spread. The Information Technology and Innovation Foundation (ITIF) noted that the number of countries enacting data localization requirements has nearly doubled from 35 in 2017 to 62 in 2021.³⁸

New obligations to keep user data in local computing facilities have recently gone into force in China, India, Turkey and Vietnam. More data localization proposals are in the legislative pipeline in numerous countries, including Bangladesh, Indonesia, Pakistan and South Africa. Some national governments force internet service providers to route data packets sent between users in their jurisdictions across networks located only within their jurisdictions. In terms of enforcement, they repeatedly issue fines against international platforms for their failure to comply with data localization rules.³⁹

Most of these local storage requirements are sector-specific or focus on a particular type of data. The regulations frequently target designated social media platforms, corporate records, health, financial or payments data.

Tracking local data protection rules becomes increasingly challenging

According to Digital Policy Alert, online privacy rules are the single most active regulatory field affecting the digital economy.⁴⁰ Importantly, consumer-protecting data privacy rules are not necessarily a hindrance to the free flow of data. Significant cross-market differences in privacy-related operating rules, together with a lack of regulatory interoperability across jurisdictions can, however, impede the free flow of data.

Countries differ strongly on what data custodians may do with personal data, what data they can ask for, how long they can hold it, who they can share it with, what they need consent for and in what form, whether it matters if the individual is a minor and what criteria define a minor in the first place. Perhaps most important are the differences in and lack of practical guidance on how to empower individuals to make informed decisions on what data they agree to share when consent is required.

The pressure on international data custodians stems from contradicting obligations between jurisdictions to protect personal data from one

country while providing access to it to law enforcement agencies in another country. Also, data custodians need to ensure equal protection abroad at the risk of potentially sizeable fines. In the case of some privacy-related cross-border data flow disputes, lack of clarity about data handling requirements can complicate compliance. Clearer and more effective regulatory coordination in the cross-border application of data privacy regulations would help address some of these challenges. The OECD declaration on government access to personal data held by the private sector can help in this regard.⁴¹ With data protection rules, conditions on cross-border data flows multiply.

While cross-border data transfer faces important sector-specific stipulations, most rules relate to the transfer of or access to personal data from abroad. Having cut through the different data protection obligations, how equal or comparable protection can be established also differs by country or region.

Options range from official recognition of jurisdiction-specific privacy standards to private certification mechanisms, binding contractual clauses between the data handling companies and explicit authorization by the supervisory body. A data custodian active in several countries may well need several ways to establish compliance with several different local privacy standards, even though its practices were universally adequate to begin with.

TABLE 1 Examples of frameworks for cross-border data transfer

Category	Description	Selected examples
Adequacy decisions	An adequacy decision by a data protection authority signifies that a foreign country provides an adequate level of data protection, allowing for the free flow of personal data between the two jurisdictions. The adequacy decision eliminates the need for any additional safeguards by the data custodians.	The European Union's General Data Protection Regulation (GDPR) empowers the European Commission to identify countries that offer an adequate level of data protection. The process also involves the European Data Protection Board and representatives of EU member states. Other countries also empower their data protection authorities to identify foreign countries that provide equivalent protections. These include the United Kingdom's Information Commissioner's Office, Japan's Personal Information Protection Commission and the Republic of Korea's Personal Information Protection Commission.
Contractual arrangements	Certain jurisdictions permit the transfer of personal data abroad if the exporter and importer enter into contractual arrangements that impose strict data handling and storing requirements on the parties. These obligations often require several compliance steps and ongoing monitoring. Given the broad range of jurisdictions that allow international data transfers through contractual arrangements, organizations are often left with a maze of contractual obligations to maintain.	The most commonly used transfer mechanisms for organizations operating at a global scale include standard contractual clauses , which are formulations for contract provisions approved and issued by the European Commission to support compliance with the GDPR. Close to Europe, organizations seeking to transfer data outside of the United Kingdom can use an international data transfer agreement (IDTA) , the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers.
Intra-firm transfers	Certain regions allow for international transfers of personal data within a corporate group if the transfers are based on regulator-approved frameworks. These frameworks are often comprised of various elements, including internal legal agreements, policies, trainings and audits. Gaining regulatory approval for these frameworks can be complicated and is often a multi-year process.	GDPR allows for international transfers within a corporate group on the basis of binding corporate rules (BCRs) , which are a set of internal agreements and policies that regulate data handling, training requirements and the like. Often, organizations utilize the EU BCRs to organize their global data privacy compliance. Other jurisdictions that recognize BCRs include Brazil, Singapore, South Africa and the United Kingdom.
Certification mechanisms	Although a relatively nascent practice, some jurisdictions allow for international data transfers when the importer is certified by an approved body or data privacy authority.	The Asia-Pacific Economic Cooperation's (APEC) cross-border privacy rules (CBPR) provide a government-backed data privacy certification that organizations can seek to demonstrate compliance. APEC CBPR certificates are currently recognized by eight countries.
User consent	International data transfers can often be made on the basis of the user's consent. The standard for consent varies across jurisdictions, generally requiring a high level of disclosure and clear options for the user to provide informed consent for the transfer. As a transfer mechanism, relying solely on consent can be challenging to scale, given the need for consent to be unambiguous, informed, and specific to a particular processing activity.	Brazil, the EU and many other jurisdictions allow for data transfer on the basis of user consent. The standard for each varies, as do the obligations that come with reliance on such a transfer mechanism.

Governments are keenly aware of the pressing need for regulatory cooperation to foster interoperability. Over the last two years, cross-border data transfers were part of the negotiations on two dozen digital trade agreements as well as several law enforcement cooperation initiatives and cross-border data flow frameworks. Recently, a number of countries participating in the APEC Cross-Border Privacy Rules (CBPR) system, including Australia, Canada, Japan, Mexico, Singapore and the US have established a Global CBPR Forum, which provides a mechanism for national data privacy certifications to be cross-recognized in a first-of-its-kind international exchange, helping to bridge different regulatory approaches to data protection and privacy. Overall, however, the arrangements for recognizing adequate data protection remain patchy, including between the G7 economies.

Consistent approaches to user consent can pre-empt fragmentation

The recent movement of many jurisdictions to enforce the consent obligations and requirements of local regulations are leading to legal fights over interpretation of the spirit of those laws. Aligning on approaches to educating and empowering users with control in consistent ways will reduce the risk of years of legal battles and confusing and inconsistent precedents around the world.⁴²

Cybersecurity risks raise the exposure to international data breaches

The final regulatory challenge for international data custodians is the compliance requirements related to the prevention and resolution of data breaches. Cybersecurity authorities are requiring localization of sensitive data – relating to critical infrastructure or banking, or geospatial information, for instance – and are seeking immediate physical access to the information infrastructure. As with data protection rules, countries differ in what pre-emptive measures they require from data handlers. Security certificates and standards are often risk-based, and therefore rarely interoperable across borders. Also, the compliance processes and notification requirements are often country-specific.

As noted above, cross-border data flows are critical to entities' cybersecurity readiness. Conversely, data flow restrictions and localization requirements impede visibility of cybersecurity risks, not only at the intra- and inter-organizational levels, but also at national and international levels. If cyber defenders cannot access threat indicators or other cybersecurity data collected in one jurisdiction, it becomes harder to address malicious activity in other jurisdictions.

Data flow restrictions and localization requirements can also impede cross-border collaboration, information sharing and coordinated network defense. When cyber defenders are thus isolated from each other, they cannot adopt a unified and coordinated defensive posture against malicious actors who do not respect local legal requirements.



3.2 The impact of regulatory fragmentation

Regulatory fragmentation creates business uncertainty

Research shows that companies are facing a range of barriers to operationalizing cross-border data flows due to global regulatory fragmentation. A recent report by Japan's Ministry of Economy, Trade and Industry, based on interviews with private-sector companies, has identified the following barriers: a) overlapping regulations within countries, which may be caused by digital silos among domestic regulators; b) lack of legal transparency resulting from multilayered regulatory requirements; c) lack of legal stability due to frequent changes in requirements and related research costs for companies; d) insufficient understanding among regulators of the business realities of cross-border data flows; e) significant costs associated with obtaining certification for data use; and f) lack of clear definitions of "cross-border flows", "personal data" and other concepts.⁴³

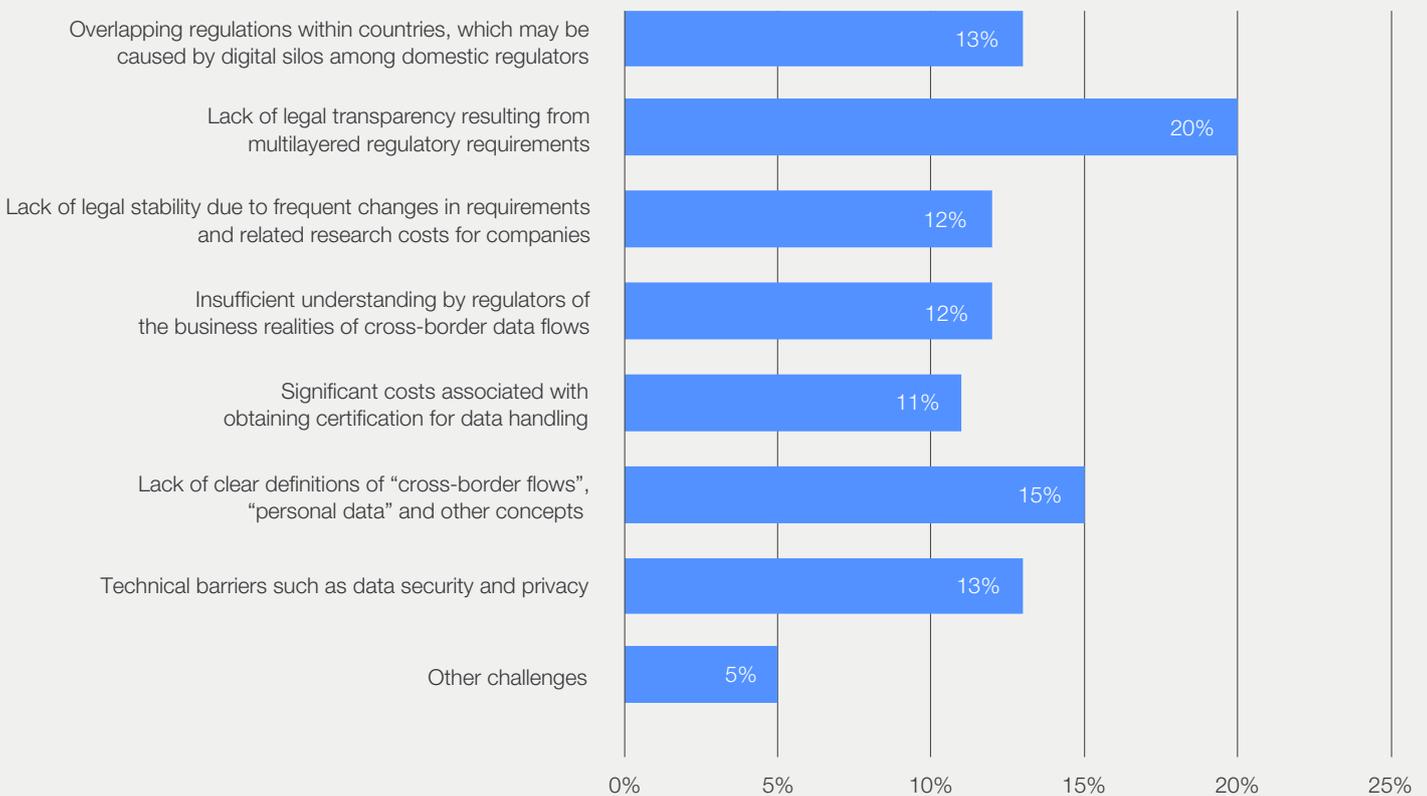
The World Economic Forum conducted a survey of SMEs around the world to gain an in-depth understanding of these challenges. The preliminary survey, based on responses from about 200 SMEs, revealed that the lack of legal transparency resulting from multilayered regulatory requirements is the most

critical issue for SMEs (Figure 1). The survey also found that in addition to the six challenges mentioned above, technical barriers such as data security and data privacy are also a major challenge for SMEs.

The other challenges identified include: customer legal requirements (e.g. a ban on offshoring of government data), data localization obligations for some Asian jurisdictions, the challenge of balancing know-your-customer/anti-money laundering (KYC/AML) obligations with data protection regulations, and integration of systems.

Regulatory fragmentation further raises compliance risk when firms are unsure about the scope and interpretation of novel regulatory regimes. For example, the European court's Schrems II decision has created uncertainty about EU-US data transfers for firms of all sizes. In fact, after the decision, US companies even outside of the tech sector have begun issuing warnings to their investors about the possible revenue hit from the court decision and conducted discussions about whether they should replace the existing businesses at some point due to the uncertainty.⁴⁴ More broadly, one survey reported that even during the pandemic (in March 2020), businesses listed regulations as one of their top concerns.⁴⁵

FIGURE 1 Major challenges SMEs face with regard to cross-border data flows



Source: World Economic Forum's internal survey on SMEs Data Readiness, 2023.



Regulatory fragmentation hits SMEs particularly hard

One particular risk with regulatory fragmentation is that it hurts the inclusive promise of a global digital economy. Thanks to the internet, every SME can create a global export market for itself just by setting up an online shop. According to a UPS survey of nine different markets, e-commerce is a top priority in SME owners' plans for growing their business at home and abroad.⁴⁶ Unfortunately, regulatory fragmentation hits SMEs particularly hard. While large multinationals may have the means to track and implement data protection, cybersecurity and cross-border transfer rules across their markets, an SME owner may simply be on her own.

When asked about policy support in growing their online business, between 20% and 50% of owners answering the UPS survey ranked simplification of e-commerce regulations as their highest priority. Almost universally shared was the challenge of learning about and complying with digital laws and regulations (60-80% of participants).

Regulatory fragmentation challenges exports, innovation and global growth

The accumulated effects of these kinds of opportunity costs and growing regulatory fragmentation between countries are significant. Restrictions on cross-border data flows, as well as complex and misaligned regulatory frameworks, can complicate the export process for businesses, increasing the costs, efforts and time spent, thereby slowing growth. One recent study found that regulatory barriers related to privacy, data storage for clients outside their home countries and consumer protection rules were some of the greatest challenges for online exporters.⁴⁷ A recent OECD study confirmed this perception and found a negative relationship between increased digital regulatory heterogeneity and parcel shipments, though it did not provide the size of the economic effect.⁴⁸ Small businesses that sell and export online were particularly impacted by these impediments, with many firms worried about the impact of data localization and complicated consumer protection

rules as potential barriers to sales. Other studies also suggest that regulatory fragmentation reduces innovation and technology diffusion.⁴⁹

Differing domestic approaches to data governance and digital trade are resulting in a web of global regulations that is becoming ever more restrictive and complex to navigate. According to a 2018

joint study by the International Federation of Accountants and the OECD's Business and Industry Advisory Committee, regulatory fragmentation can cost the global economy more than \$780 billion annually. These costs can be more harmful for SMEs that are not as well-resourced as their larger counterparts.⁵⁰



3.3 Interoperability to address regulatory fragmentation

The right of societies to regulate an enormously important entity such as the digital economy through, for example, data privacy laws impedes international agreement on a single regulatory approach. A less intrusive approach would preserve domestic regulatory discretion while minimizing fragmentation of the trading system through regulatory interoperability.

International trade has always been regulated when products being traded present challenges to important public policy objectives such as protecting public or animal health, public security or environmental sustainability. When it comes to the ingredients in our food, the safety standards for our vehicles or what technologies may or may not be sold across borders, governments have never ceded their right to regulate to an international forum. Rather, such issues have been subject to mutual recognition agreements, with countries bilaterally recognizing equivalence between the standards or the integrity of certification systems. For the same reasons, it may be impractical for governments to harmonize their approaches to the cross-border transfer of data by delegating rule-making to an international standard setter. The public interest in privacy and the need

for safeguarding sensitive national security or financial data limit what citizens may allow their representatives to do.

As the digital economy expands, governments are increasingly grappling with how best to manage and benefit from the digital transformation while at the same time safeguarding the broader public interest. As a result, new rules related to privacy, cybercrime and cybersecurity are proliferating. To add to the complexity, policy-makers' motivations for regulatory intervention can differ across jurisdictions. According to the Institute of International Finance, governments intervene for a variety of reasons, including in support of law enforcement and privacy protection.⁵¹ These rules can impede cross-border data flows, and, in turn, stymie growth opportunities for vulnerable SMEs.

The digital economy is a uniquely dynamic and innovative sector. Entirely new regulatory fields such as artificial intelligence or blockchain technology can appear and grow exponentially with breathtaking speed. Regulators, therefore, need to be nimble and have the ability to adjust rapidly to fast-paced changes in their domestic digital ecosystems.

The opportunity to institutionalize DFFT

4.1 Challenges for regulatory interoperability

The free flow of data across borders is critical to the modern digital economy. Enhancing the international interoperability of domestic data privacy and protection rules is a key enabler for the free flow of data. The international system already provides two mechanisms for increasing regulatory interoperability: trade or economic partnership agreements, and recognition of foreign data rules. Enabling the interoperability of national data regulations and standards through existing mechanisms, however, is a complex and potentially daunting undertaking.

Trade agreements can be a powerful mechanism to increase interoperability between differing national data protection rules, but their reach remains limited. At the multilateral level, the General Agreement on Trade in Services (GATS) of the World Trade Organization (WTO) is one such mechanism. In cases where countries have made specific commitments under GATS, they are obligated to keep their markets open to the relevant service suppliers. The applicability of GATS to data flows, however, remains strongly contested. Even if it were applicable, GATS' impact on the free flow of data would likely be limited. Its binding commitments differ by signatory, are sector-specific and remain subject to security and general exceptions for measures necessary for protecting public morals or privacy.

The existing and currently under-negotiation agreements at the plurilateral and bilateral levels share GATS characteristics. While they include specific provisions for the free flow of data, they generally allow for similar exceptions as those available under GATS. Signatories may thus attach conditions to the free flow of data for national security, public safety or similar reasons.

Recognition of foreign data rules can also be a powerful mechanism to increase interoperability, but few international recognition decisions have been taken so far. In principle, governments can recognize foreign data rules in three ways: through adequacy decisions for individual countries, by recognizing international frameworks or by recognizing certificates that demonstrate firm-level compliance with a specified data protection standard.

Since they only involve designated countries, individual adequacy decisions are a limited approach to increasing interoperability worldwide. For a more sizeable increase in regulatory interoperability, governments could recognize an international privacy framework that all signatories would uphold. Several candidates exist for such an international privacy framework, including the Council of Europe's Convention 108, the OECD Privacy Guidelines, the ASEAN Personal Data Protection Framework, the APEC Privacy Framework and the Malabo Convention. However, apart from Convention 108, none of these is legally binding on participating governments. Without binding and enforceable commitments, the recognition of an international privacy framework is highly unlikely. Finally, governments could increase regulatory interoperability by directly recognizing certified business standards. Some candidates here are the APEC CBPR and ISO/IEC standards 27001/27701 from the International Organization for Standardization (ISO). To date, these certificates have only been recognized by a few governments.

Increasing mutual trust and opening communication channels could help address some of these concerns. First, countries need strong understanding of each other's rules and trust in each other's frameworks before they can recognize each other's approaches through individual decisions or through binding trade agreement provisions. They must also be mindful of their cultural and legal differences.

Building trust through a new institutional mechanism can counter the underlying issues holding back the existing mechanisms and presents an opportunity to accelerate regulatory interoperability between national data rules.

These include, but are not limited to:

- 1 Limited reach of trade agreements.
- 2 Contested scope and applicability of international legal rules, including in trade agreements.
- 3 Few international recognition decisions.
- 4 Non-legally binding international privacy frameworks (such as the OECD Privacy Framework and the APEC Privacy Guidelines).
- 5 Limited coverage of firm-level compliance certificates.

4.2 | New momentum to collaborate on cross-border data flows

The momentum between governments to cooperate to address digital issues is increasing. For instance, OECD member countries and the European Union signed the Declaration on Government Access to Personal Data Held by Private Sector Entities on 14 December 2022, the first inter-governmental document to facilitate government access to personal data held by private companies for law enforcement purposes while safeguarding privacy.⁵²

More specifically in the DFFT context, the Japanese government recently proposed the creation of an “Institutional Arrangement for Partnership (IAP)” among the G7 this year. In a recent speech, Japan’s Minister for Digital Transformation, Kono Taro, described the IAP as a vehicle where “policy experts, companies, universities and other entities with real knowledge and experience can develop and implement specific projects that will turn the DFFT into reality.”

In addition to government stakeholders, private sector participants increasingly recognize the

importance of an institutional framework of public and private collaboration for cross-border data flows. In line with the Japanese government’s proposal, the London Stock Exchange Group (LSEG) recently supported “(t)he establishment of a G7-led forum to strengthen international coordination on data and digital governance.” LSEG says that the G7 should coordinate with private sector stakeholders to provide practical inputs and should seek to promote some activities including those ensuring transparency.⁵³ Additionally, the Institute for International Finance, a global association with 400 members from 60 countries, has recognized the need for a new strategic framework for digital cooperation, stating that the world is at an inflection point and a new framework is needed to “hammer out the new rules for a digital world.”⁵⁴

As efforts to get governments and other stakeholders to work together to advance DFFT gather steam, it is time to take collective action towards establishing an institutional mechanism to address global challenges for cross-border data flows.

4.3 | The unique potential of a new institutional mechanism

According to the OECD, the regulatory environment must facilitate digitalization for its benefits to be realized.⁵⁵ However, the current multilateral or regional forums are not positioned to coordinate across institutions, international forums and governments to promote interoperability of regulations in various jurisdictions. A new coordinating body to improve international communication, processes and outcomes on data flows is needed to help inform and shape coherent cross-border data governance policies

and to promote interoperability. A new institutional mechanism could help advance DFFT and catalyse regulatory interoperability through the coordination of existing mechanisms globally.

If designed carefully, an institutional mechanism would complement existing mechanisms and be an important and strategic venue where stakeholders could exchange knowledge, develop evidence and case studies, share best practices and pilot practical solutions that increase interoperability.

A well-designed new mechanism would convene diverse perspectives, maintain focus on the most pressing obstacles to interoperability yet avoid the high stakes of trade agreement negotiations, formal dispute settlement proceedings, or mutual recognition decisions. Building momentum through incremental solutions, such a mechanism could become a catalyst for progress and make an important, novel contribution to increasing the interoperability of national data governance systems.

The new mechanism would help create consistency and accountability through continuous collaboration and gathering of shared experience. As officials confer regularly, they benefit from trust-building and cooperation, which catalyses long-term thinking for sustainable solutions beyond short-term fixes. Establishing short communication channels between like-minded governments, regulators and domain experts is a highly valuable asset on its own, but particularly so to coordinate in an international crisis.

BOX 3

Call to action

This paper encourages the G7 governments to aim for a **permanent** new institutional mechanism that convenes senior government officials and **high-level** representatives of multiple stakeholder groups. It should be **empowered to test** new ideas and practical steps to increase

interoperability. Importantly, such a mechanism would **complement, not supplant, the existing international groups** covering these issues. This call for action should carry forward to the G20 and beyond.

This paper recommends that this new institutional mechanism focus on operationalizing the DFFT and have a permanent secretariat to support governments towards this end, ensuring continuity across G7 presidencies. It should institutionalize multistakeholder engagement including not only senior regulators and policy-makers but also recognized experts from non-governmental organizations (NGOs), international organizations, businesses and academia. Such broad-based engagement is critical to helping governments prioritize issues as well as understanding and promoting the utilization of technology to achieve policy goals. It would also raise the constructive creativity of this new institutional mechanism so it can identify practical proposals and respond rapidly to changes in the digital economy.

Respecting the inherent national differences, an institutional mechanism would serve as a convening forum for government officials to meet regularly to assess gaps, define key challenges and work towards practical solutions to promote interoperability between their respective data governance systems. A permanent, multistakeholder institutional mechanism that can test practical approaches to operationalizing DFFT can become a vehicle to accelerate progress towards increased interoperability. By providing a space for transparent discussions and collaborative experimentation, the venue can foster mutual understanding and trust between stakeholders, ultimately accelerating the spread of recognition and the development of interoperable data privacy and protection standards. Conceived in this way, the new institutional mechanism would play a key role in fuelling progress through existing mechanisms in the global system and increase interoperability within the G7 and beyond.

As a further design choice, the new institutional mechanism should be equipped with the resources needed to create a laboratory for new ideas and novel solutions with potentially global reach. Guided by the issues identified through multistakeholder discussions, governments can set priorities. The secretariat can then launch projects to develop and test practical solutions to incrementally advance interoperability. It could thus support interoperability of data rules across jurisdictions without interference in domestic regulations. These core concepts can help advance a global environment where data flows can contribute to innovation, resilience, inclusion and economic growth, while prioritizing data privacy, security, consumer empowerment and trust in cross-border digital ecosystems. In designing the institutional mechanism, intergovernmental and multistakeholder collaboration would be helpful to identify challenges and priorities as well as to develop proposals to address them.

In summary, establishing an institutional mechanism with a permanent secretariat focused on promoting the free flow of data with trust would be a critical contribution to the global system governing the rapidly evolving global digital economy. Its permanence and multistakeholder approach would create accountability and trust, providing a forum for regulators, policy-makers, NGOs, international organizations, businesses, academia and other stakeholders to work together towards ensuring free flow of data while respecting national differences in regulatory approaches.

Main purpose

A new institutional mechanism would help advance Data Free Flow with Trust (DFFT) and serve as an important accelerator to increase interoperability through the coordination of existing mechanisms.

Key benefits

- 1 Support interoperability of data rules across jurisdictions without interference in domestic regulations.
- 2 Provide a laboratory for practical ideas and solutions to incrementally advance data free flow.

- 3 Secure voice, ideas and ownership for diverse stakeholders including government, labour, business and civil society.

- 4 Create consistency, short communication channels and accountability among its participants.

Design

- 1 A permanent secretariat (for continuity and support).
- 2 Multistakeholder engagement (for helping governments prioritize issues).
- 3 Resources to develop and test practical solutions.



Conclusion

The ongoing growth and expansion of the digital economy brings challenges. Governments around the world are weighing how best to manage the benefits of digital transformation against the imperative of protecting the broader public interest across an array of issues. Policy-makers must find ways to encourage innovation, while advancing policies that protect consumers and their data without stifling growth. At the same time, the development and spread of emerging technologies will look for ever-increasing cross-border data flows to fuel continuing innovation and growth.

The global data policy landscape is becoming increasingly complex. While often well intentioned, regulations are being introduced that can restrict the free movement of data across borders. These regulations can unintentionally raise costs for businesses, harm innovation and adversely impact consumers. In addition, the global regulatory landscape is becoming fragmented, further amplifying complexity and having other negative impacts.

In 2019, the then Japanese prime minister, Shinzo Abe introduced the DFFT concept to facilitate cross-border data flows, recognizing the importance of trust and respecting different regulatory approaches. Since then, the need for DFFT has only become more pronounced. The COVID-19 pandemic boosted the digital economy.

Today, people, businesses, governments and civil society all recognize the importance of digital tools and data flows for economic resilience and inclusion. The widespread availability and adoption of digital technologies has enabled greater appreciation of the importance of data and cross-border data flows to support continued innovation across all sectors.

To help realize the DFFT vision, the 2023 G7 meetings present an opportunity to secure commitments for an institutional mechanism – or an Institutional Arrangement for Partnership (IAP). Such an arrangement would bring together government officials, experts from international organizations and other stakeholders to advance DFFT.

It would encourage regulatory interoperability and ensure the success of cross-border data flows. By anchoring data in trust, and enabling data to flow freely across borders, the Institutional Arrangement for Partnership would benefit all stakeholders including users, businesses, governments and civil society. It would go beyond the search for short-term fixes and catalyse long-term thinking for sustainable solutions to operationalize DFFT, thereby advancing the global digital economy and supporting the economic growth and general welfare of all.

Contributors

This initiative is a multi-industry, multistakeholder endeavour. This paper is a combined effort based on numerous discussions between all stakeholders. However, the opinions expressed herein may not necessarily correspond with those of each individual involved with the project listed below.

Lead authors

Todd Fox

Head of Global Policy, Visa

Johannes Fritz

CEO, St. Gallen Endowment for Prosperity Through Trade

Satoru Hori

Chief Researcher & Unit Manager, Hitachi

Tomoaki Nakanishi

Executive Director, Japan External Trade Organization (JETRO), San Francisco, USA; Fellow, World Economic Forum

Michael Nunes

Head of Government Advisory, Visa

Supheakmungkol Sarin

Head of Data & AI Ecosystems, World Economic Forum

Acknowledgements

Mohammed AlEidan

Lead, Data Management, Saudi Aramco; Fellow, World Economic Forum

Flavia Alves

Head of International Institutions and Relations, Meta

Karla Yee Amezaga

Lead, Data Policy, World Economic Forum

Kimmy Bettinger

Lead, Expert and Knowledge Communities, World Economic Forum

Sebastian Buckup

Deputy Head of Centre for the Fourth Industrial Revolution, World Economic Forum

Julien Chaisse

Professor, School of Law, City University of Hong Kong

Tenzin Chomphel

Project Coordinator, Data Policy, World Economic Forum

Jennifer Cosco

Global Head of Government Relations & Regulatory Strategy, LSEG (London Stock Exchange Group)

Javier Ruiz Diaz

Senior Advisor, Consumers International

Michael DiPaula-Coyle

Head of International Trade Policy, IBM Corporation

Daniel Dobrygowski

Head, Governance and Trust, World Economic Forum

Ziyang Fan

Head of Digital Trade, World Economic Forum

Rashmi Gupta

Partner, IBM Corporation

Hollie Hamblett

Policy Specialist, Consumers International

Noboru Koshizuka

Professor, The University of Tokyo; Chair, Data Society Alliance

Fumiko Kudo

Project Strategy Lead, Centre for the Fourth Industrial Revolution Japan

Hosuk Lee-Makiyama

Director, European Centre for International Political Economy (ECIPE)

Clara Lemaire

European Government Affairs Director, Splunk Inc

Cathy Li

Deputy Head of Centre for the Fourth Industrial Revolution, World Economic Forum

Allan Millington

Global Data Policy Leader, Data Office, EY

Shigehiro Muraki

Head of Administration, Centre for the Fourth Industrial Revolution Japan

Didier Navez

Senior Vice President, Data Policy & Governance, Dawex

Mio Otashiro

Deputy Consul General of Japan in Auckland, New Zealand; Fellow, World Economic Forum

Syed Iftikhar Hussain Shah

Digital Research Director, Digital Cooperation Organization (DCO)

Jonathan Soble

Editorial and Communication Lead, Centre for the Fourth Industrial Revolution Japan

Luke Stafford

Manager, Government Relations & Regulatory Strategy, LSEG (London Stock Exchange Group)

Kati Suominen

Founder & CEO, Nextrade Group

Sergio A. VeLarde

Senior Privacy Counsel, Visa

Stefaan Verhulst

Co-Founder of The GovLab (NYC) and The Data Tank (Brussels)

Priya Vithani

Platform Curator, Data Policy, World Economic Forum

Joseph Whitlock

Executive Director, Global Data Alliance; Director, Policy, BSA | The Software Alliance

Yoshitaka Yamamuro

Head, Centre for the Fourth Industrial Revolution Japan

Xiao Yan

Project Lead, Digital Trade International Trade and Investment, World Economic Forum

We also would like to thank the members of the World Economic Forum's task force on Data Free Flow with Trust for all their insights and contributions.

Endnotes

1. James Sullivan, "The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks: Why They Matter", Tradeology, 2019, <https://blog.trade.gov/2019/09/13/the-eu-u-s-and-swiss-u-s-privacy-shield-frameworks-why-they-matter/>.
2. Daniel S. Hamilton and Joseph P. Quinlan, "The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe", 2022, https://transatlanticrelations.org/wp-content/uploads/2022/03/TE2022_report_HR.pdf.
3. Organisation for Economic Co-operation and Development (OECD), "Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies", 2019, <https://doi.org/10.1787/276aaca8-en>.
4. Shah Syed Iftikhar Hussain, Abdulaal Alaa and Peristeras Vassilios, "Data divide in digital trade, and its impacts on the digital economy: A literature review", Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance (ICEGOV '22), 432-439, 2022, <https://doi.org/10.1145/3560107.3560173>.
5. World Economic Forum, "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows", 2020, https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf.
6. World Economic Forum, "'Defeatism about Japan is now defeated': Read Abe's Davos speech in full", 2019, <https://www.weforum.org/agenda/2019/01/abe-speech-transcript/>.
7. Ministry of Foreign Affairs of Japan, "G20 Ministerial Statement on Trade and Digital Economy", 2019, <https://www.mofa.go.jp/files/000486596.pdf>.
8. Ministry of Foreign Affairs of Japan, "G20 Osaka Leaders' Declaration", 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.
9. The government of the United Kingdom, "Ministerial Declaration G7 Digital and Technology Ministers' meeting", 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/981567/G7_Digital_and_Technology_Ministerial_Declaration.pdf.
10. The government of Germany, "Ministerial Declaration, G7 Digital Ministers' meeting", 2022, <https://www.bundesregierung.de/resource/blob/998440/2038510/e8ce1d2f3b08477eeb2933bf2f14424a/2022-05-11-g7-ministerial-declaration-digital-ministers-meeting-en-data.pdf?download=1>.
11. The White House, "G20 Bali Leaders' Declaration", 2022, <https://www.whitehouse.gov/briefing-room/statementsreleases/2022/11/16/g20-bali-leaders-declaration/>.
12. Organisation for Economic Co-operation and Development (OECD), "Cross-Border Data Flows: Taking Stock of Key Policies and Initiatives", 2022, <https://doi.org/10.1787/5031dd97-en>.
13. Asia-Pacific Economic Cooperation (APEC), "2022 Leaders' Declaration", 2022, <https://www.apec.org/meeting-papers/leaders-declarations/2022/2022-leaders-declaration>.
14. Ministry of Economy, Trade and Industry of Japan, "G20 Digital Economy Minister's Meeting on September 1, 2022, Remarks by Nagamine Makoto, Parliamentary Vice-Minister of Economy, Trade and Industry, Japan", 2022, <https://www.meti.go.jp/press/2022/09/20220902002/20220902002-1.pdf>.
15. Center for Strategic and International Studies (CSIS), "Leading Japan's Digital Transformation: A Discussion with Kono Taro", 2023, <https://www.csis.org/events/leading-japans-digital-transformation-discussion-kono-taro>.
16. Javier López González, Francesca Casalini and Juan Porras, "A Preliminary Mapping of Data Localisation Measures", OECD Trade Policy Papers, No. 262, 2022, <https://doi.org/10.1787/c5ca3fed-en>.
17. World Bank, "World Development Report 2021: Data for Better Lives", 2021, <https://www.worldbank.org/en/publication/wdr2021>; United Nations Conference on Trade and Development, "Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow", 2021, <https://unctad.org/webflyer/digital-economy-report-2021>.
18. United Nations Conference on Trade and Development, "Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow", 2021, <https://unctad.org/webflyer/digital-economy-report-2021>.
19. Daniel S. Hamilton and Joseph P. Quinlan, "The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe", 2022, https://transatlanticrelations.org/wp-content/uploads/2022/03/TE2022_report_HR.pdf.
20. Daniel Ker and Emanuele Mazzini, "Perspectives on the value of data and data flows", OECD Digital Economy Papers, No. 299, 2020, https://www.oecd-ilibrary.org/science-and-technology/perspectives-on-the-value-of-data-and-data-flows_a2216bc1-en.
21. World Economic Forum, "Shaping the Future of Digital Economy and New Value Creation", 2020, <https://www.weforum.org/centres-and-platforms/shaping-the-future-of-digital-economy-and-new-value-creation>.
22. OECD, "Leveraging digital trade to fight the consequences of COVID-19", 2020, https://read.oecd-ilibrary.org/view/?ref=135_135517-02bikxyksj&title=Leveraging-Digital-Trade-to-Fight-the-Consequences-of-COVID-19.
23. Barbara Kotschwar, Sakina Lavingia and Mike Nunes, "Global economic cooperation: Writing the rules for the digital economy", Visa Economic Empowerment Institute, 2022, <https://usa.visa.com/content/dam/VCOM/regional/na/us/sites/documents/veei-global-economic-cooperation.pdf>.

24. OECD, “Leveraging digital trade to fight the consequences of COVID-19”, 2020, https://read.oecd-ilibrary.org/view/?ref=135_135517-02bikxyksj&title=Leveraging-Digital-Trade-to-Fight-the-Consequences-of-COVID-19.
25. Francesca Casalini and Javier López González, “Trade and Cross-Border Data Flows”, OECD Trade Policy Papers, No. 220, 2019, <https://doi.org/10.1787/b2023a47-en>.
26. Dubai Future Foundation, “Future Opportunities Report – The Global 50”, 2023, <https://www.dubaifuture.ae/the-global-50>.
27. Bhaskar Chakravorti, Ajay Bhalla and Ravi Shankar Chaturvedi, “Which economies showed the most digital progress in 2020”, Harvard Business Review, 2020, <https://hbr.org/2020/12/which-economies-showed-the-most-digital-progress-in-2020>.
28. OECD, “Mapping Approaches to Data and Data Flows”, 2020, <https://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf>.
29. Visa Economic Empowerment Institute, “Helping the hardest hit: Recovery and resilience for small business in the United States”, 2021, <https://usa.visa.com/content/dam/VCOM/global/ms/documents/veei-us-small-business-in-the-digital-age.pdf>.
30. Visa Economic Empowerment Institute, “Small Business in the Digital Age: Dubai MSMEs: Digital and resilient”, 2022, <https://usa.visa.com/content/dam/VCOM/regional/na/us/sites/documents/veei-dubai-small-business-in-the-digital-age.pdf>; Visa Economic Empowerment Institute, “Small Business in the Digital Age: Transforming for global reach: Small business in the UK”, 2022, <https://usa.visa.com/content/dam/VCOM/regional/na/us/sites/documents/veei-uk-transforming-for-global-reach.pdf>.
31. Todd Fox and Barbara Kotschwar, “From access to opportunity: Digital skills drive women’s economic empowerment”, Visa Economic Empowerment Institute, 2023, <https://usa.visa.com/content/dam/VCOM/regional/na/us/sites/documents/veei-from-access-to-opportunity.pdf>.
32. World Bank, “Crossing Borders”, 2021, <https://wdr2021.worldbank.org/stories/crossing-borders/>.
33. Neira Hajro, Klemens Hjartar, Paul Jenkins and Benjamim Vieira, “What’s next for digital consumers”, McKinsey, 2021, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/whats-next-for-digital-consumers>.
34. VISA, “Consent Management Guidelines”, <https://globalclient.visa.com/consentmanagement>.
35. Global Data Alliance, “Automotive”, <https://globaldataalliance.org/sectors/automotive/>.
36. Experian, “Experian and Oliver Wyman find expanded data and advanced analytics can improve access to credit for nearly 50 million credit invisible and unscorable Americans”, 2022, <https://www.experianplc.com/media/latest-news/2022/experian-and-oliver-wyman-find-expanded-data-and-advanced-analytics-can-improve-access-to-credit-for-nearly-50-million-credit-invisible-and-unscorable-americans/>; Experian, “Meet the 5 million ‘credit invisible’ Brits still at risk of exclusion from the financial system”, 2022, <https://www.experianplc.com/media/latest-news/2022/meet-the-5-million-credit-invisible-brits-still-at-risk-of-exclusion-from-the-financial-system/>.
37. Digital Policy Alert, “Data governance”, <https://digitalpolicyalert.org/policy-area/data-governance>; Sara Marcucci, Natalia Gonzalez Alarcon, Stefaan G. Verhulst and Elena Wullhorst, “Mapping and Comparing Data Governance Frameworks: A benchmarking exercise to inform global data governance deliberations”, 2023, <https://arxiv.org/abs/2302.13731>.
38. Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them”, Information Technology and Innovation Foundation, 2021, <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>.
39. Digital Policy Alert, “Activity Tracker”, <https://digitalpolicyalert.org/activity-tracker>.
40. Digital Policy Alert, Activity Tracker, 2023: <https://digitalpolicyalert.org/activity-tracker>.
41. OECD, “Declaration on Government Access to Personal Data Held by Private Sector Entities”, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.
42. Kelvin Chan, “European Union fines Facebook parent Meta 390M euros for privacy violations”, PBS NewsHour, 2023, <https://www.pbs.org/newshour/world/european-union-fines-facebook-parent-meta-390m-euros-for-privacy-violations>.
43. Ministry of Economy, Trade and Industry of Japan, “Interim Report of the Expert Group on Data Free Flow with Trust”, 2022, https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2e.pdf.
44. Sam Sabin, “As Officials Hash Out Deal to Replace Privacy Shield, More Companies — Beyond Tech — Warn Investors About the Risk”, Morning Consult, 2021, <https://morningconsult.com/2021/04/20/privacy-shield-compliance-sec-filings/>.
45. Federal Reserve Bank of Atlanta, “Survey of Business Uncertainty”, 2023, <https://www.atlantafed.org/research/surveys/business-uncertainty>.
46. UPS, “Supporting SMB Growth: Unlocking Recovery through E-commerce”, 2021, <https://about.ups.com/content/dam/upsstories/assets/our-stories/customer-first/ups-survey-understands-smbs/SMBResearchFullReport.pdf>.
47. Kati Suominen, “The CPTPP’s Impacts on Digital Trade and the Path Forward”, Center for Strategic and International Studies (CSIS), 2021, <https://www.csis.org/analysis/cptpps-impacts-digital-trade-and-path-forward>.
48. Javier López González and Silvia Sorescu, “Trade in the Time of Parcels”, OECD Trade Policy Papers, No. 249, 2021, <https://doi.org/10.1787/0faac348-en>.
49. Rebecca Janßen, Reinhold Kesler, Michael E. Kummer and Joel Waldfoegel, “GDPR and the Lost Generation of Innovative Apps”, National Bureau of Economic Research, Working Paper 30028, 2022, <https://doi.org/10.3386/w30028>; Jian Jia, Ginger Zhe Jin and Liad Wagman, “The Short-Run Effects of GDPR on Technology Venture Investment”, National Bureau of Economic Research, Working Paper 25248, 2018, <https://doi.org/10.3386/w25248>.

50. International Federation of Accountants (IFAC) and Business and Industry Advisory Committee at the OECD (BIAC), "Regulatory Divergence: Costs, Risks and Impacts", 2018, <https://www.ifac.org/system/files/publications/files/IFAC-OECD-Regulatory-Divergence.pdf>.
51. Conan French, Brad Carr and Clay Lowery, "Data Localization: Costs, Tradeoffs, and Impacts Across the Economy", Institute of International Finance, 2020, https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.
52. OECD, "Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access", 2022, <https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm>.
53. London Stock Exchange Group, "Unlocking the value of data flows in the digital economy", 2022, https://www.lseg.com/content/dam/lseg/en_us/documents/policies/unlocking-the-value-of-data-flows-in-the-digital-economy.pdf.
54. Institute of International Finance, "Strategic Framework for Digital Economic Cooperation", 2021, https://www.iif.com/portals/0/Files/content/Innovation/10_11_2021_digital_economic_cooperation.pdf.
55. Taku Nemoto and Javier López González, "Digital trade inventory: Rules, standards and principles", OECD Trade Policy Papers, No. 251, 2021, <https://doi.org/10.1787/9a9821e0-en>.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org