

Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows

BRIEFING PAPER
JANUARY 2023



Contents

3	Introduction
4	1 Data Free Flow with Trust (DFFT)
5	2 Policy and business challenges
5	2.1 The policy angle
6	2.2 The business perspective
7	3 Recent policy processes and available tools
7	3.1 The policy layer
8	3.2 The tool layer
9	4 Call to action
9	4.1 Institutional mechanism
9	4.2 Business tools for interoperability and beyond
10	5 Conclusion
11	Contributors
12	Endnotes

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.

Introduction

The movement of data across country borders is essential to the global economy – carrying information and enabling innovation, value and wealth. When data flows across borders, it is possible to deliver more to more people and produce more benefits for people and planet.

Many countries are putting forward regulations to constrain data flow in order to deal with the challenges of privacy, national security and intellectual property, or for economic reasons such as protecting domestic jobs. Such restrictions, even if well-intentioned, can lead to regulatory fragmentation and challenges for business, especially when combined with data localization requirements. If undermined, this could ultimately weaken global trade flows and limit the societal benefits for all. Unfortunately, the current fragmented approach has stalled (or even potentially set back) policy efforts to implement frameworks for cross-border data flows.

This paper highlights the importance of such data flows and urges global leaders in the public and private sectors to take collective action to work towards a shared understanding of them with a view to implementing “Data Free Flow with Trust” (DFFT) – an umbrella concept for facilitating trust-based data exchanges – through policy mechanisms and concrete tools for businesses. However, it is important to note that the paper focuses mainly on business-to-business (B2B) data transfers across borders.

The aim is not to provide a definitive or exhaustive list of policy recommendations and tools that can address the immediate and long-term challenges. Rather, it is to review the current challenges facing DFFT, take stock of progress made so far, offer direction for policy mechanisms and concrete tools for businesses and, more importantly, promote global discussions about how to realize DFFT from the perspectives of policy and business.

1

Data Free Flow with Trust (DFFT)

Global data traffic reached 230 exabytes, or 230 billion gigabytes, per month in 2020 and is forecast to more than triple, to reach up to 780 exabytes per month, by 2026.¹

Digital trade has been the fastest-growing area of global trade over the past decade, growing by 5.4% each year on average and contributing more to global growth than the trade in goods.² One study shows that by 2023 cross-border B2B commerce is expected to account for two-thirds of digital trade (\$1.78 trillion).³

For global businesses, recent research led by Japan's Ministry of Economy, Trade and Industry (METI) identified a range of industries and operations that involve cross-border data transfers. They include: a) providers and developers of online apps; b) transfer of data to an overseas outsourcer; c) real-time data collection and analysis from other countries via the internet of things (IoT); d) provision of platform services and internet as a service; and e) cybersecurity services. For instance, by using an IoT platform to collect and analyse

real-time data on utilities' operating conditions, operating environments, repairs, etc., for devices sold globally, the companies will be able to predict the occurrence of failures and produce optimized maintenance plans based on such data.⁴ In short, activities in these areas produce essential products and services that enhance people's quality of life.

Cross-border data policies must respond to these economic and social impacts while being mindful of the importance of securing trust. At the G20 in 2019, Japanese prime minister Shinzo Abe declared the launch of the "Osaka Track" on "Data Free Flow with Trust" (DFFT), a vision for data flows in which openness and trust in data flows coexist and complement each other.⁵

In fact, members of the G7 countries have recognized that "DFFT underpins innovation, prosperity and democratic values".⁶ This vision has also been carried forward to the latest G20 in Bali, where the G20 Bali Leaders' Declaration clearly mentioned, "We remain committed to further enable data free flow with trust and promote cross-border data flows."⁷

BOX 1

Multistakeholder approach to cross-border data flows

In parallel with the policy dialogue at the intergovernmental level, there have also been active discussions among multistakeholders to help and complement intergovernmental dialogues regarding cross-border data policies through public and private partnership. For instance, the World Economic Forum published DFFT-related white papers, "Exploring International Data Flow Governance", "A Roadmap for Cross-Border Data Flows",* "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows" and "Rebuilding Trust and Governance:

Towards Data Free Flow with Trust (DFFT)", with the aim of helping policy-makers move forward with DFFT while involving multiple stakeholders.^{8, 9, 10, 11}

* Recommendations from these multistakeholder approaches include: a) allow data to flow by default; b) establish a level of data protection; c) prioritize cybersecurity; d) hardwire accountability between nations; e) prioritize connectivity, technical interoperability, data portability and data provenance; and f) future-proof the policy environment.¹²

2

Policy and business challenges

Despite ongoing discussions to advance DFFT, the political reality and landscape remains a patchwork of national regulations based on objectives on economic development, protection of privacy, and other human rights and national security concerns.¹³

The resulting geopolitical fragmentation and approaches to policy present challenges to fully realizing DFFT.

2.1 The policy angle

Data policies vary widely with regard to the cross-border transfer of personal data, but can be categorized into three basic models: (1) open safeguards; (2) pre-authorized safeguards; and (3) limited transfers.^{14, 15} These models may eventually

converge, but the current diversified landscape of policies and regulations creates costs, operational complexity and uncertainties for businesses and other entities seeking to share data across borders.

TABLE 1 Cross-border data transfer models

Open safeguards	Approaches that tend to leave discretion as to how to safeguard transfers to the private sector, often on the basis of public guidelines. They include private-sector adequacy, contracts and ex-post accountability.
Pre-authorized safeguards	Mechanisms under which public-sector approval is required prior to transfer based on a series of transparent criteria. These include public-sector adequacy and other ex-ante legal instruments such as contractual clauses or binding corporate rules.
Limited transfers	These impose strict and less transparent requirements on cross-border flows of data for companies and other organizations, and may include case-by-case and ad-hoc authorization by the government following a security assessment. They often include a condition for storing and sometimes processing personal data within the country of origin. Limited transfers can often apply to less well-defined categorizations of data such as “important” or “critical” data.

A recent OECD report shows that a growing number of countries are adopting data localization rules – explicit requirements 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

The economic effect of those data localization rules is alarming. For instance, according to an Information Technology & Innovation Foundation (ITIF) report, several studies show that data localization and other barriers to data flows impose

significant economic costs in several countries: “reducing U.S. GDP by 0.1-0.36 percent; causing prices for some cloud services in Brazil and the European Union to increase 10.5 to 54 percent; and reducing GDP by 0.7 to 1.7 percent in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam”.¹⁷ Another piece of research from Frontier Economics shows that the difference between a path that is moderately liberalizing and one that is moderately restrictive is worth a little over 1.5% in EU GDP per year, which is equivalent to approximately one year of GDP growth for the EU according to the IMF’s long-run forecasts.¹⁸

2.2 The business perspective

In the context of global regulatory fragmentation and rising data localization, research efforts have shown that companies are facing a range of barriers.^{19, 20, 21} One of the most recent efforts is the METI's report, based on interviews with the private sector.²²

The report 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 by regulators of the business realities of cross-border data flows; e) significant costs associated with obtaining certification for data handling; and f) lack of clear definitions of "cross-border flows", "personal data" and other concepts.

TABLE 2 Cross-border data transfers and business pain points

Types of cross-border data transfers	Examples of business pain points
1 Product development by online app companies	– Barriers to entry are too high for start-ups and SMEs as laws and regulations vary from country to country
2 Transfer to a foreign third-country company for outsourcing	– Unclear if data integration and data access among multiple regions across borders constitute a "cross-border transfer" – Companies are required to ensure the same protection and management systems in the destination country as in the source country when transferring data across borders to a third country
3 Real-time data analysis from abroad via IoT¹ devices – no personal data is included	– Growing regulations on non-personal data as new data categories such as "security information" emerge. Often vague in scope and prone to sudden change – Case-by-case review processes for data localization rules could undermine the advantages of real-time monitoring, a basic capability of IoT
4 Real-time data analysis from abroad via IoT devices – personal data is included	– "Personal data" definitions extend not only to laws but also to guidelines and administrative notices, making them difficult to implement and interpret
5 Provide platform services and IaaS²	– Requirements for cross-border transfers are highly complex, necessitating frequent customer agreements
6 Providing cybersecurity services	– Region-specific certifications may be required for security-related information, in addition to global rules and standards, imposing a significant cost burden

Notes: 1. IoT (internet of things); 2. IaaS (internet as a service)

Source: Fumiko Kudo, Ryosuke Sakaki and Jonathan Soble, "Every Country Has Its Own Digital Laws. How Can We Get Data Flowing Freely between Them?", World Economic Forum, 2022: <https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/>

BOX 2 Examples of barriers to cross-border data flows

(Taken from "Issues from the Company's Perspective" in the METI report, p. 10.)

One company stated that the definition of and provisions governing the cross-border transfer of "personal data", which extend not only to the main text of the regulations but also to the guidelines and administrative agreements, are difficult to interpret.²³ Another company commented that

when data is transferred across borders to a third country, businesses are asked to ensure that their counterparts provide the same level of protection in their data management system and operation as the data-origin country even though the counterparts are in a different regulatory jurisdiction; abiding by these regulations puts a disproportionate burden and responsibility on businesses.

It is hoped that such barriers will ultimately be eased through bilateral agreements, deliberations at the G7 and G20, and dialogue at other international organizations. Since it will likely take time to address these barriers, businesses also need tools to

navigate today's differing regulatory approaches and instruments, and to mitigate the risks associated with cross-border data flows.

3

Recent policy processes and available tools

3.1 The policy layer

As a recent Organisation for Economic Co-operation and Development (OECD) report described, many existing agreements, processes and initiatives seek to promote trusted cross-border data flows.²⁴ Countries have developed a range of policies and regulations to unilaterally govern the flow of data across borders in an effort to establish trust. In addition, a range of processes in intergovernmental

fora have helped advance cooperation. These include: a) deliberations by the G7 and the G20; b) standard-setting efforts and research and analysis initiatives promoting dialogue in multilateral organizations; c) standard-setting or binding agreements among regional partners; and d) a variety of preferential trade agreements.

TABLE 3 Policy process for cross-border data flows

<p>Unilateral policies and regulations</p>	<p>Domestic approaches that enable the transfer of certain types of data to countries outside the domestic territory under certain conditions:²⁵</p> <ul style="list-style-type: none"> – Open safeguards: these rely primarily on the transferring entity to ensure the continued protection of the public policy objectives involved without being generally prescriptive as to how these requirements must be met – Pre-authorized safeguards: these are generally characterized by a greater involvement of the public sector ex-ante to ensure trusted data transfers. They include: the required incorporation into contracts of specific clauses preapproved by the public sector; the public sector’s preapproval of organizations’ binding corporate rules; or domestic certification schemes
<p>Intergovernmental-level processes</p>	<ul style="list-style-type: none"> – Deliberations by the G7 and the G20 – Multilateral approaches <ul style="list-style-type: none"> – Standard-setting efforts and research and analysis initiatives promoting dialogue among multilateral organizations (e.g. OECD, United Nations, World Trade Organization, World Bank) – Regional arrangements <ul style="list-style-type: none"> – Standard-setting or binding agreements among regional partners (e.g. Asia-Pacific Economic Cooperation [APEC], Association of Southeast Asian Nations [ASEAN], the European Union [EU]) – Preferential trade agreements <ul style="list-style-type: none"> – Treaties that remove barriers to trade and set rules for international commerce between two countries or among a small group of countries²⁶ (e.g. Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP], EU-UK Trade and Cooperation Agreement, UK-Singapore Digital Economy Agreement)

At the G7 summit in Germany in 2022, digital ministers considered DFFT as one of six ministerial-level points of discussion and adopted a “G7 Action Plan Promoting Data Free Flow with Trust”. This includes: a) strengthening the evidence base for DFFT; b) building on commonalities in order to foster future interoperability; c) continuing regulatory cooperation; d) promoting DFFT in the context of digital trade; and e) sharing knowledge about the prospects for international data spaces.²⁷

In the same year, at the G20 summit in Indonesia, the chair’s summary of the G20 Digital Economy Ministers’ Meeting described the importance of further work to identify “commonalities, complementarities, and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability”.²⁸

3.2 The tool layer

Along with these policy discussions, technological, legal and other tools have been developed to mitigate the business risks associated with data-sharing and to promote smoother cross-border data flows.

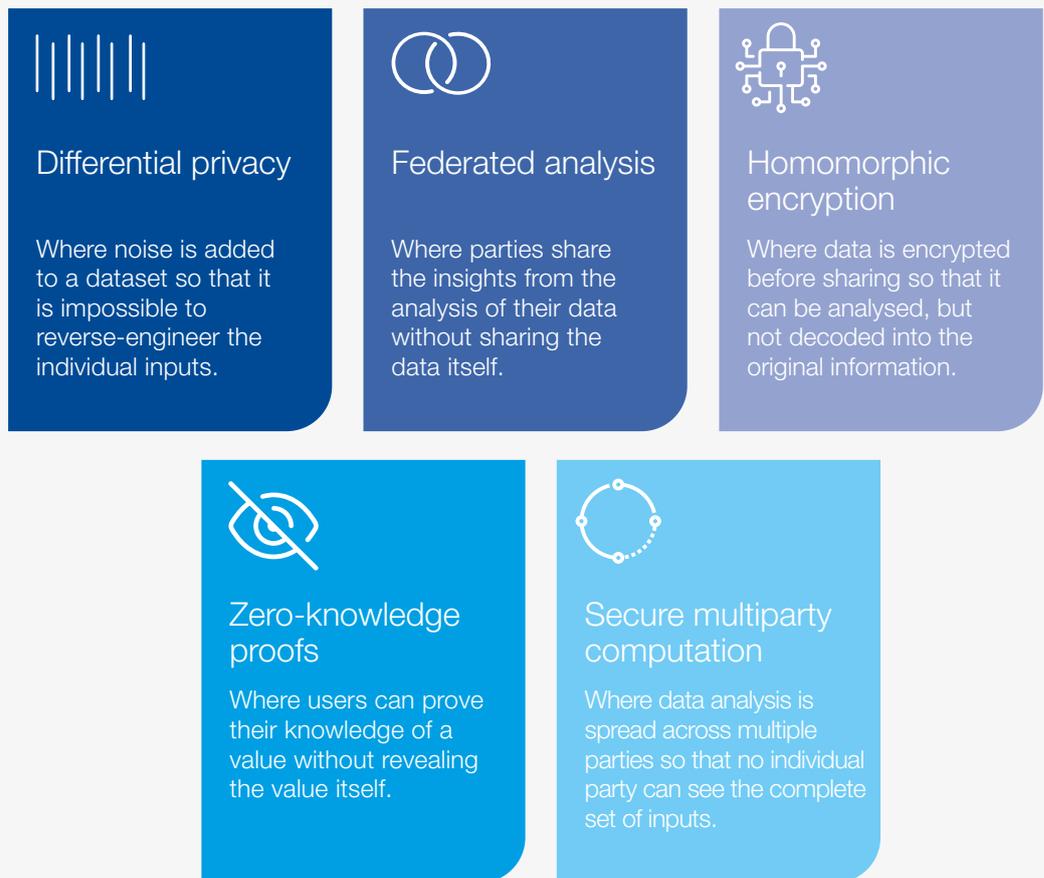
One tool to mitigate legal risk and reduce compliance costs is the use of model or standard contractual clauses for cross-border data transfers. Authorities have developed clauses that are recommended or even required for contracts between entities seeking to share data across borders. When incorporated into contracts, these clauses are automatically considered sufficient for the lawful transfer of data. Examples are “Standard Contractual Clauses” for data transfers between EU and non-EU countries²⁹ and “ASEAN Model Contractual Clauses for Cross-Border Data Transfers” for data transfers between ASEAN nations.³⁰

An additional tool to mitigate legal risk and reduce compliance costs is the deployment of data marketplaces operated by data marketplace service

providers. These bring capabilities to conduct trusted data transactions more efficiently, providing traceability, security and compliance with regulations. Data marketplace operators, acting as neutral trusted third parties and data exchange experts, can also assist parties engaged in cross-border data exchanges, in regards to evolving regulations, reducing the burden of risk assessments.

Another set of tools consists of privacy-enhancing technologies/techniques (PETs). PETs are technological measures that have the potential to fundamentally redefine the dynamics of data-sharing by eliminating or greatly reducing the risks associated with collaboration.³¹ They include: a) differential privacy; b) federated analysis; c) homomorphic encryption; d) zero-knowledge proofs; and e) secure multiparty computation. Though each technique has its limitations and needs to be researched further, PETs have the potential to facilitate cross-border data flows while ensuring regulatory compliance.

FIGURE 1 Key techniques for managing data privacy



Source: World Economic Forum, “The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value”, 2019

Those tools will likely be more powerful for businesses as more countries will authorize and standardize them for cross-border data flows. This

will require more policy dialogue that involves all relevant actors.

4

Call to action

What are the logical next steps to realize DFFT?

As mentioned above, the chair's summary of the 2022 G20 Digital Economy Ministers' Meeting described the need to work towards identifying "commonalities, complementarities, and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability".³² Given the regulatory fragmentation around the

globe, securing interoperability among existing approaches and instruments at the international level is the basic direction of actions that policy-makers and other stakeholders can take now. Based on this understanding, solutions should include both an institutional mechanism to secure interoperability at the international level and practical tools for global businesses to mitigate the risk and cost of moving data across borders.

4.1 Institutional mechanism

Given the regulatory fragmentation, the next step in the policy layer should be for the G7 countries, in collaboration with international organizations, to establish an institutional mechanism with the aim of securing interoperability by coordinating measures to enable smoother and more coherent data flows between countries, including those with differing data-protection approaches, while protecting trust.^{33, 34}

At the same time, discussions across other fora should also be encouraged to continue –whether at the OECD, at the G20 under the Digital Economy Working Group or the Trade and Investment Working Group, or in the World Trade Organization (WTO) – in the context of the Joint Statement

Initiative on E-commerce. It will be important that these cut across policy silos, including in the digital and trade communities.

In the long term, it will be possible to expand the functions of the institutional mechanism, once established, which will then cover not only the facilitation of data transfers across borders but also the development of global governance framework to unlock the value of data for the common good while protecting trust. In order to develop a cross-border governance framework, there needs to be further discussion among multistakeholders at the international level in terms of accountability, transparency and representation.

4.2 Business tools for interoperability and beyond

As mentioned, standard or model contractual clauses for cross-border data transfers as a legal tool and PETs as a technological tool are being developed for global businesses to mitigate the risk and cost of moving data across borders, given the existing differences in regulations. Other technological tools, such as data marketplaces and a standardized interface that allows organizations to share specific data safely, should be developed further to foster interoperability and facilitate cross-border data flows.

Another potential approach is to develop a repository for cross-border data transfer regulations to improve the transparency of rules, on the assumption that the regulations are different in each region. This would be a highly accessible repository for cross-border data transfer regulations, through application programming interfaces (APIs) and a better-visibility user interface. If developed, it would allow users to explore, track and analyse the different regulatory approaches, and it would make all of the regulations

it contains available in machine-readable format through an API. In addition, the repository would not only facilitate compliance for the private sector but also encourage the public sector to initiate regulatory dialogue with other countries by using it as a foundation for the dialogue.

Moreover, granular data classification could also be an option. This approach can reduce costs through more targeted risk profiling and compliance requirements. Developing simple and standardized ways to classify business data with granularity would help companies avoid the tendency to see all data as "sensitive", a situation that hinders cross-border data flows, allowing some data to be unlocked not only for commercial purposes but also for the public good.

While establishing granular data classification is not an easy task, it would be valuable to increase efforts to agree on a common taxonomy of data types through multistakeholder approaches at the international level.³⁵

5

Conclusion

The global data policy landscape remains complex and will likely become only more so as a growing number of countries adopt data localization practices; what is worse, such data localization measures are becoming more restrictive. Taking collective actions to mitigate the costs and risks caused by geopolitical fragmentation and to fully realize DFFT is thus needed now, otherwise DFFT is likely to remain a vision that will never materialize.

This paper proposes, therefore, that public-private collaboration is required to fully realize DFFT by overcoming complex geopolitical fragmentation

through building and enhancing trust. Public-private partnerships, gathering expertise and wisdom around the globe, should result in the creation of an effective and trusted mechanism to foster further interoperability while also developing concrete tools for businesses to mitigate the risk and cost of moving data across borders.

The authors hope that this paper will provide a valuable contribution to the discussion among policy-makers and other stakeholders as they design new cross-border data governance models.



Contributors

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

Lead authors

Tomoaki Nakanishi

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

Satoru Hori

Senior Researcher, Hitachi America; Fellow, World Economic Forum

Co-authors

Nada Al-Saeed

Executive Director of Strategy and Research, Bahrain Economic Development Board

Julien Chaisse

Professor, School of Law, City University of Hong Kong

Tenzin Chomphel

Project Coordinator, Data Policy, World Economic Forum

Ziyang Fan

Head of Digital Trade, World Economic Forum

Noboru Koshizuka

Professor, Interfaculty Initiative in Information Studies, The University of Tokyo

Fumiko Kudo

Project Strategy Lead, Centre for the Fourth Industrial Revolution Japan

Takuya Kudo

Partner, McKinsey & Company

Javier López González

Senior Economist, Trade and Agriculture Directorate, Organisation for Economic Co-operation and Development

Didier Navez

Senior Vice-President, Strategy and Alliances, Dawex

Supheakmungkol Sarin

Head of Data & AI Ecosystems, World Economic Forum

Stefaan G. Verhulst

Co-Founder, The GovLab, Tandon School of Engineering, New York University

Gabriela Zanfira-Fortuna

Vice-President for Global Privacy, Future of Privacy Forum

Acknowledgements

We would like to thank the following individuals for their contributions of time and insights to this paper: Jonathan Soble, Kimmy Bettinger, Priya Vithani, Yoshitaka Yamamuro and Sebastian Buckup.

Endnotes

1. 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>.
2. Zurich Insurance, “Cross-Border Data Flows: Designing a Global Architecture for Growth and Innovation”, 2022: <https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation>.
3. Daniel S. Hamilton and Joseph 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.
4. Ministry of Economy, Trade and Industry, “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.
5. 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>.
6. G7, “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>.
7. The White House, “G20 Bali Leaders’ Declaration”, 2022: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/16/g20-bali-leaders-declaration/>.
8. World Economic Forum, “Exploring International Data Flow Governance”, 2019: <https://www.weforum.org/whitepapers/exploring-international-data-flow-governance>.
9. World Economic Forum, “A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy”, 2020: <https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy/>.
10. World Economic Forum, “Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows”, 2020: <https://www.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows/>.
11. World Economic Forum, “Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT)”, 2021: <https://www.weforum.org/whitepapers/rebuilding-trust-and-governance-towards-data-free-flow-with-trust-dfft/>.
12. World Economic Forum, “A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy”, 2020: <https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy/>.
13. 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>.
14. World Bank, “Crossing Borders”, 2021: <https://wdr2021.worldbank.org/stories/crossing-borders/>.
15. 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>.
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. Nigel Cory, “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?”, Information Technology & Innovation Foundation, 2017: <https://www2.itif.org/2017-cross-border-data-flows.pdf>.
18. Frontier Economics, “The Value of Cross-Border Data Flows to Europe: Risks and Opportunities”, 2021: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf.
19. 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>.
20. 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>.
21. 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>.
22. Ministry of Economy, Trade and Industry, “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.
23. Ibid.
24. 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>.
25. Francesca Casalini, Javier López González and Taku Nemoto, “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers”, OECD Trade Policy Papers, no. 248, 2021: <https://doi.org/10.1787/ca9f974e-en>.

26. Congressional Budget Office, “How Preferential Trade Agreements Affect the U.S. Economy”, 2016: <https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/reports/51924-tradeagreements.pdf>.
27. G7, “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>.
28. G20, “G20 Digital Economy Ministers’ Meeting 2022: Chair’s Summary”, 2022: <https://www.g20.org/wp-content/uploads/2022/10/G20-DEMM-Chairs-Summary.pdf>.
29. European Commission, “Standard Contractual Clauses (SCC)”, 2021: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
30. Association of Southeast Asian Nations, “ASEAN Model Contractual Clauses for Cross Border Data Flows”, 2021: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
31. World Economic Forum, “The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value”, 2019: <https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value/>.
32. G20, “G20 Digital Economy Ministers’ Meeting 2022: Chair’s Summary”, 2022: <https://www.g20.org/wp-content/uploads/2022/10/G20-DEMM-Chairs-Summary.pdf>.
33. 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>.
34. Julien Chaisse, “‘The Black Pit’: Power and Pitfalls of Digital FDI and Cross-Border Data Flows”, World Trade Review, 2022.
35. 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>.



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